Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik, 55133 Bonn

Per Mail
Dienststellen der obersten Bundesbehörden
Ressort-IT-Sicherheitsbeauftragte – o. V. i. A.

ITZ Bund (ISB)

Landes-CISOs über Geschäftsstelle der AG InfoSic

Geschäftsstelle BLK

[redacted]
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn

Postanschrift:
Postfach 20 03 06
53133 Bonn

Tel. +49 228 99 9582-[redacted]
Fax +49 228 99 10 9582-[redacted]

poststelle@bsi-bund.de-mail.de

www.bsi.bund.de

**Betreff: Mindeststandards nach § 8 BSIG**
hier: Nutzung externer Cloud-Dienste

Bezug: Mein Schreiben – B 12 – 750-00-07 vom 27.04.2017
Geschäftszeichen: BL35 - 750 00 07
Datum: 20.11.2020

Anlage:-1 - Entwurf Mindeststandard „MST-NCD-RfC-Beta-1.0.5.docx“
-2- Änderungstabelle „MST-NCD-RfC-Beta-Abgleich-V1.0.5.docx“

Mit Bezugsschreiben hatte ich die Version 1.0 des Mindeststandards zur Nutzung externer Cloud-Dienste veröffentlicht. Seit dem konnten insbesondere in Beratungsgesprächen Konkretisierungen und Änderungsbedarfe identifiziert werden. Neben weiteren formalen Anpassungen wird der Mindeststandard daher im Rahmen des Lifecycle-Management-Prozesses überarbeitet, so dass er im 1. Quartal 2021 als Major-Release in der Version 2.0 veröffentlicht werden kann. Eine BSI-Interne Abstimmung hat dazu bereits stattgefunden.

Im Rahmen des nun anstehenden Konsultationsverfahrens ist es mir wichtig, die Fachexpertise von IT-Verantwortlichen, IT-Sicherheitsbeauftragten, IT-Betriebspersonal und IT-Beschaffern einzuholen. Gerne können Sie daher den Entwurf auch in Ihrem Zuständigkeitsbereich entsprechend weiterleiten.

Weiterhin liegt diesem Schreiben eine Änderungstabelle bei, die die Regelungstexte der Version 1.0 und der zu kommentierenden Version 1.0.5 gegenüberstellt. Dies soll die Kommentierung und Rückmeldung erleichtern.

Die wichtigsten Änderungen habe ich für den ersten Überblick nachfolgend aufgeführt:
- Anforderungen zur Mitnutzung von externen Cloud-Diensten sind jetzt im Kapitel 2.5 aufgeführt. Der bisher eigenständig geführte Mindeststandard zur Mitnutzung externer Cloud-Dienste entfällt mit der Veröffentlichung der neuen Version 2.0.
- Der jährliche Informationsaustausch zum 31.01. ist entfallen. Eine Meldung zum 31.01.2021 ist daher bereits nicht mehr erforderlich.
- Der Anwendungsbereich in Kapitel 1 ist konkretisiert. Hier liegt jetzt der Fokus insbesondere auf der Verarbeitung von dienstlichen Daten.

- Die Sicherheitsanforderungen sind an den neuen Kriterienkatalog Cloud Computing des BSI (C5:2020) angepasst.
- Die Sicherheitsanforderungen sind mit dem IT-Grundschutz-Baustein OPS.2.2 „Cloud Nutzung“ stärker verzahnt.
- Modal-Verben analog IT-Grundschutz-Kompendium werden in den Sicherheitsanforderungen durchgängig genutzt.

Die Mindeststandards nach § 8 BSIG sind ein wichtiger Bestandteil zur Erreichung und Sicherung des IT-Sicherheitsniveaus in der Bundesverwaltung. Gemeinsam mit Ihnen möchten wir daher die Sicherheitsanforderungen stetig hinsichtlich ihrer Praxisrelevanz überprüfen und weiterentwickeln. Kommentierungen und Rückmeldungen richten Sie bitte bis zum 08. Januar 2021 per Email an das Postfach mindeststandards@bsi.bund.de. Wenn sie bereits während der Kommentierung Rückfragen haben, stehen die Kolleginnen und Kollegen des Referates BL 35 „Mindeststandards Bund“ gerne zur Verfügung.

Mit freundlichen Grüßen
Im Auftrag

Samsel

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

# Mindeststandard des BSI zur Nutzung externer Cloud-Dienste

nach § 8 Absatz 1 Satz 1 BSIG – RfC-Beta-Version 1.0.5 vom 17.11.2020

# Änderungshistorie

| *Version* | *Datum* | *Beschreibung* |
|---|---|---|
| 1.0 | 24.04.2017 | Erstveröffentlichung |
| 1.0.1 | 13.07.2020 | RfC-Alpha-Version, Rohentwurf auf Basis der Delta-Dokumentation |
| 1.0.2 | 25.09.2020 | Prüfung, Überarbeitung und Freigabe durch Fachreferat |
| 1.0.3 | 29.09.2020 | RfC-Alpha-Version zur hausinternen Abstimmung |
| 1.0.4 | 09.11.2020 | Kommentare und Rückmeldungen aus der hausinternen Abstimmung eingearbeitet |
| 1.0.5 | 17.11.2020 | Ressorts erhalten Entwurf zur Kommentierung |

Tabelle 1: Versionsgeschichte des Mindeststandards. Eine ausführliche Änderungsübersicht zum Mindeststandard erhalten Sie unter: https://www.bsi.bund.de/mindeststandards (**Hinweis:** wird vor Release konkretisiert)

Bundesamt für Sicherheit in der Informationstechnik Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6262
E-Mail: mindeststandards@bsi.bund.de
Internet: https://www.bsi.bund.de

# Vorwort

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes auf der Grundlage des § 8 Abs. 1 BSIG. Als gesetzliche Vorgabe definieren Mindeststandards ein konkretes Mindestniveau für die Informationssicherheit. Der Umsetzungsplan Bund 2017 legt fest, dass die Mindeststandards des BSI auf Basis § 8 Abs. 1 BSIG zu beachten sind.[1] Die Definition erfolgt auf Basis der fachlichen Expertise des BSI in der Überzeugung, dass dieses Mindestniveau in der Bundesverwaltung nicht unterschritten werden darf. Der Mindeststandard richtet sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe)[2] und IT-Betriebspersonal.

IT-Systeme sind in der Regel komplex und in ihren individuellen Anwendungsbereichen durch die unterschiedlichsten (zusätzlichen) Rahmenbedingungen und Anforderungen gekennzeichnet. Daher können sich in der Praxis regelmäßig höhere Anforderungen an die Informationssicherheit ergeben, als sie in den Mindeststandards beschrieben werden. Aufbauend auf den Mindeststandards sind diese individuellen Anforderungen in der Planung, der Etablierung und im Betrieb der IT-Systeme zusätzlich zu berücksichtigen, um dem jeweiligen Bedarf an Informationssicherheit zu genügen. Die Vorgehensweise dazu beschreiben die IT-Grundschutz-Standards des BSI.

Zur Sicherstellung der Effektivität und Effizienz in der Erstellung und Betreuung von Mindeststandards arbeitet das BSI nach einer standardisierten Vorgehensweise. Zur Qualitätssicherung durchläuft jeder Mindeststandard mehrere Prüfzyklen einschließlich des Konsultationsverfahrens mit der Bundesverwaltung.[3] Über die Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich jede Stelle des Bundes auch bei der Erschließung fachlicher Themenfelder für neue Mindeststandards einbringen oder im Hinblick auf Änderungsbedarf für bestehende Mindeststandards Kontakt mit dem BSI aufnehmen. Einhergehend mit der Erarbeitung von Mindeststandards berät das BSI die Stellen des Bundes[4] auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Vgl. Umsetzungsplan Bund 2017 (BMI 2017), S. 4
[2] Analog „Informationssicherheitsbeauftragter (ISB)“
[3] Siehe FAQ zu den Mindeststandards (BSI 2020)
[4] Zur besseren Lesbarkeit wird im weiteren Verlauf für „Stelle des Bundes“ der Begriff „Einrichtung“ verwendet.

# Inhalt

# 1 Beschreibung

Dieser Mindeststandard setzt Sicherheitsanforderungen an die Nutzung externer Cloud-Dienste. Die Erfüllung der im Mindeststandard vorgegebenen Sicherheitsanforderungen ist für ein angemessenes IT-Sicherheitsniveau notwendig, aber in der Regel nicht hinreichend. Unter Berücksichtigung des individuellen Schutzbedarfs muss die Festlegung und Umsetzung eventuell zusätzlich erforderlicher Sicherheitsanforderungen erfolgen. Er richtet sich hinsichtlich seiner Umsetzung an IT-Sicherheitsbeauftragte, IT-Betriebs- und Fachverantwortliche.[5]

## 1.1 Begriffsbestimmung und Abgrenzung

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Insbesondere werden dabei Infrastrukturen, Plattformen und Software angeboten, die Spannbreite der angebotenen Cloud-Dienste umfasst darüber hinaus jedoch das komplette Spektrum der Informationstechnik.[6]

Externe Cloud-Dienste im Sinne dieses Mindeststandards sind im Rahmen von Cloud Computing angebotene Dienstleistungen, die über Netze und Anbieter der Wirtschaft außerhalb der öffentlichen Verwaltung des Bundes und der Länder erbracht werden.[7]

Als Nutzung ist eine Verarbeitung von dienstlichen Daten[8] durch einen externen Cloud-Dienst zu verstehen, der durch die Einrichtung selbst oder gemeinsam mit anderen beauftragt wird. Werden externe Cloud-Dienste durch Benutzer[9] einer Einrichtung lediglich mitgenutzt, regelt Kapitel 2.5 den Umgang mit dienstlichen Daten in diesen Fällen entsprechend. Von einer Mitnutzung wird insbesondere ausgegangen, wenn die Einrichtung den externen Cloud-Diensten nicht beauftragt hat.

Werden keine dienstlichen Daten verarbeitet, können die Regelungen des Mindeststandards trotzdem angewendet werden (siehe NCD.2.1.03, Buchstabe e)).

## 1.2 Modalverben

In Anlehnung an den IT-Grundschutz[10] werden die Sicherheitsanforderungen mit den Modalverben MUSS und SOLLTE sowie den zugehörigen Verneinungen formuliert. Darüber hinaus wird das Modalverb KANN für ausgewählte Prüfaspekte verwendet. Die hier genutzte Definition basiert auf RFC 2119[11] und DIN 820-2: 2018[12].

**MUSS / DARF NUR**

bedeutet, dass diese Anforderung zwingend zu erfüllen ist. Das von der Nichtumsetzung ausgehende Risiko kann nicht im Rahmen einer Risikoanalyse akzeptiert werden.

**DARF NICHT / DARF KEIN**

bedeutet, dass etwas zwingend zu unterlassen ist. Das durch die Umsetzung entstehende Risiko kann nicht im Rahmen einer Risikoanalyse akzeptiert werden.

---

[5] Rollen nach IT-Grundschutz-Kompendium, (BSI 2020b), S.31
[6] Definition nach https://www.bsi.bund.de/cloud
[7] Hinweis: IT-Dienstleistungen der „Bundescloud“ fallen somit nicht unter diese Bestimmung.
[8] Dienstlich sind alle Daten, die im Rahmen der dienstlichen Tätigkeit erhoben und verarbeitet werden. Darunter fallen jedoch nicht personenbezogene Daten (wie Stammdaten, Nutzungsdaten), die für die Registrierung und Nutzung des Dienstes vom Cloud-Diensteanbieter erhoben oder verarbeitet werden.
[9] Analog Rolle „Benutzer“ nach IT-Grundschutz-Kompendium, (BSI 2020b), S.31
[10] Vgl. BSI-Standard 200-2 (BSI 2017), S. 18
[11] Vgl. Key words for use in RFCs (IETF 1997)
[12] Vgl. DIN-820-2: Gestaltung von Dokumenten (DIN 2018)

### SOLLTE

bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

### SOLLTE NICHT / SOLLTE KEIN

bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

### KANN

bedeutet, dass die Umsetzung / Nicht-Umsetzung optional ist und ohne Angabe von Gründen unterbleiben kann.

# 2 Sicherheitsanforderungen

Nachfolgende Sicherheitsanforderungen adressieren die Informationssicherheit entlang des gesamten Lebenszyklus und setzen auf den IT-Grundschutz-Baustein OPS.2.2 *Cloud-Nutzung*[13] auf.

## 2.1 Planungsphase

Grundlage der Informationssicherheit im Bereich Cloud Computing bilden nach dem IT-Grundschutz-Baustein OPS.2.2: *Cloud-Nutzung*

- die Cloud-Nutzungs-Strategie
- die darauf basierende Sicherheitsrichtlinie sowie
- das jeweilige Sicherheitskonzept für den externen Cloud-Dienst.

Die nachfolgenden Sicherheitsanforderungen adressieren diese Dokumente entsprechend.

**NCD.2.1.01 Cloud-Nutzungs-Strategie**

a) Die Einrichtung MUSS prüfen, ob der externe Cloud-Dienst grundsätzlich mit den in der Cloud-Nutzungs-Strategie definierten Zielen, Chancen und Risiken vereinbar ist.[14]

b) Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn Ziele, Chancen und Risiken der Cloud-Nutzungs-Strategie angemessen berücksichtigt werden können.

**NCD.2.1.02 Sicherheitsrichtlinie externe Cloud-Dienste**

a) Die Einrichtung MUSS eine Sicherheitsrichtlinie für externe Cloud-Dienste nach OPS.2.2.A2 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*[15] erstellen.

b) Die Einrichtung MUSS in dieser Sicherheitsrichtlinie mindestens die Umsetzung und Einhaltung der Basiskriterien nach dem Kriterienkatalog Cloud Computing (C5) als spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter festlegen.[16]

c) Die Einrichtung MUSS die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragen bei der Erstellung der Sicherheitsrichtlinie beteiligen.

**NCD.2.1.03 Sicherheitskonzept für den externen Cloud-Dienst**

a) Die Einrichtung MUSS ein Sicherheitskonzept für den externen Cloud-Dienst nach OPS.2.2.A7 *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung* erstellen.

b) Die Einrichtung MUSS in dem Sicherheitskonzept die aktuellen Veröffentlichungen des BSI zu Cloud-Sicherheit berücksichtigen.[17]

c) Die Einrichtung MUSS die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragen bei der Erstellung des Sicherheitskonzeptes beteiligen.

d) Die Einrichtung MUSS eine Datenkategorisierung durchführen, in der sämtliche dienstliche Daten identifiziert werden, die künftig in dem externen Cloud-Dienst verarbeitet werden sollen.

[13] IT-Grundschutz-Kompendium, (BSI 2020b), OPS.2.2: *Cloud-Nutzung*
[14] Hinweis: OPS.2.2.A1 *Erstellung einer Cloud-Nutzungs-Strategie* sieht die Erstellung einer Cloud-Nutzungs-Strategie vor. In dieser erfasst die Einrichtung ihre Ziele, Chancen und Risiken, die sie mit einer Cloud-Nutzung generell verbindet. Die Cloud-Nutzungs-Strategie nimmt daher eine zentrale Rolle für die Einrichtung ein. Sie wird benötigt, um die beabsichtigte Nutzung eines konkreten externen Cloud-Dienstes bewerten zu können.
[15] IT-Grundschutz-Kompendium, (BSI 2020b), OPS.2.2: *Cloud-Nutzung*
[16] Kriterienkatalog Cloud Computing (C5), (BSI 2020a), S.1ff.
[17] Siehe Veröffentlichungen unter https://www.bsi.bund.de/cloud

e) Kommt die Einrichtung zu dem Ergebnis, dass in dem externen Cloud-Dienst keine dienstlichen Daten verarbeitet werden, handelt es sich nicht um eine Nutzung oder Mitnutzung externer Cloud-Dienste im Sinne dieses Mindeststandards. In diesem Fällen KANN die Einrichtung die Sicherheitsanforderungen des Mindeststandards umsetzen.

f) Die Einrichtung MUSS für die identifizierten dienstlichen Daten Geheim- und Datenschutzaspekte[18] sowie Personen- und Dienstgeheimnisse ermitteln.

g) Die Einrichtung MUSS die identifizierten dienstlichen Daten den nachfolgenden Kategorien zuordnen:

- Kategorie 1 = Privat- und Dienstgeheimnisse gemäß §§ 203 und 353b StGB
- Kategorie 2 = personenbezogene Daten gemäß § 3 Absatz 1 BDSG
- Kategorie 3 = Verschlusssachen gemäß Verschlusssachenanweisung - VSA[19]
- Kategorie 4 = sonstige Daten (weder Kategorie 1, noch 2, noch 3)

h) Die Einrichtung KANN die identifizierten dienstlichen Daten den Kategorien 1, 2 oder 3 gleichzeitig zuordnen.

i) Die Einrichtung MUSS Risiken, die aus der künftigen Nutzung des externen Cloud-Dienstes entstehen können, umfassend ermitteln.[20]

i) Die Einrichtung MUSS die ermittelten Risiken mit denen in der eigenen Cloud-Nutzungs-Strategie (siehe NCD.2.1.01) festgelegten Richtlinien der Risikobewertung abgleichen und bewerten.

ii) Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn die ermittelten Risiken gemäß der in der Cloud-Nutzungs-Strategie genannten Richtlinien zur Risikobewertung wirksam vermieden oder hinreichend reduziert oder getragen werden können.

### NCD.2.1.04 Notfall- und Kontinuitätsmanagement

Mit Notfall- bzw. Kontinuitätsmanagement ist gemäß BSI-Standard 100-4[21] ein Managementsystem zur Aufrechterhaltung einer definierten Arbeitsfähigkeit einer Einrichtung gemeint und umfasst sowohl präventive als auch reaktive Maßnahmen auf Notfälle und Krisensituationen. Es gilt im weiteren die Begrifflichkeit des BSI-Standards 100-4[22].

a) Die Einrichtung MUSS prüfen, ob sie in Notfällen und Krisensituationen weiter auf den externen Cloud-Dienst zugreifen können muss. [23]

b) Die Einrichtung MUSS bewerten, welche Bedeutung der externe Cloud-Dienst in Notfällen einnehmen würde.[24]

[18] Hinsichtlich Datenschutzaspekte siehe insbesondere (AKTM 2011), S.1ff.
[19] Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), (BMI 2018)
[20] Hinweis: Bei dieser Prüfung geht es um eine anbieterunabhängige Prüfung. Es soll in diesem Zusammenhang geklärt werden, ob das beabsichtigte Cloud-Szenario mit der Cloud-Nutzung-Strategie vereinbar ist (z.B. Können die eigenen rechtlichen und organisatorischen Rahmenbedingungen überhaupt erfüllt werden?)
[21] BSI-Standard 100-4 – Notfallmanagement, (BSI 2008), S.1ff.
[22] BSI-Standard 100-4 – Notfallmanagement, (BSI 2008), S.1ff.
[23] Hinweis: Leitfragen für diese Prüfung können sein: Wird der Cloud-Dienst für einen, im Notfallmanagement als zeitkritisch bewerteten Geschäftsprozess (bzw. Fachaufgabe) genutzt? Dient der Cloud-Dienst zur Etablierung und Aufrechterhaltung eines Notbetriebs? Ist der Cloud-Dienst für die Bewältigung eines Notfalls relevant?
[24] Hinweis: Leitfragen für diese Prüfung können sein: Wie zeitkritisch sind die Geschäftsprozesse (bzw. Fachaufgaben), die den Cloud-Dienst in einem Notfall oder einer Krise benötigen? Zu welchem Grad wird der Cloud-Dienst in einem Notbetrieb benötigt?

c) Die Einrichtung MUSS den zuständigen Notfallbeauftragten entsprechend einbinden. Dieser MUSS prüfen, ob die Prävention vor bzw. die Reaktion auf Notfälle oder Krisen durch die Cloud-Nutzung geändert werden muss. Die Einrichtung MUSS diese Änderungen vor der Cloud-Nutzung umsetzen.

## 2.2 Beschaffungsphase

Ziel des Beschaffungsprozesses, für den die Vorgaben des Vergaberechts einschlägig sind, ist die Auswahl eines geeigneten Cloud-Diensteanbieters.

### NCD.2.2.01 Umsetzung der Sicherheitsanforderungen

a) Die Einrichtung MUSS vor Vertragsabschluss überprüfen, ob die in ihrer Sicherheitsrichtlinie festgelegten Sicherheitsanforderungen (siehe NCD.2.1.02, Buchstabe a)) vom Cloud-Diensteanbieter erfüllt werden können.[25]

b) Die Einrichtung MUSS diese Sicherheitsanforderungen bereits in der Leistungsbeschreibung des externen Cloud-Dienstes einfordern.

c) Die Einrichtung MUSS die Angaben und Nachweise des Cloud-Diensteanbieters zu Buchstabe a) hinsichtlich Inhalt, Aussagekraft, Nachvollziehbarkeit, Aktualität, nachteiliger Regelungen sowie Mitwirkungspflichten und Maßnahmen auswerten. Dazu SOLLTE der „*Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5*“[26] verwendet werden.

d) Die Einrichtung MUSS sich die regelmäßige Vorlage von Sicherheitsnachweisen vom Cloud-Diensteanbieter zusichern lassen.

e) Diese Sicherheitsnachweise SOLLTEN

- die angemessene und wirksame Umsetzung der Basiskriterien nach C5[27],
- die aktuelle Dokumentation der Systembeschreibung[28],
- die Aktualität von vertraglich zugesicherten Zertifizierungen sowie
- die ordnungsgemäße Durchführung von Datensicherungen und erprobten Rücksicherungen

umfassen und durch die regelmäßige Bereitstellung des aktuellen Prüfberichtes nach C5 erbracht werden. Andere Nachweise DARF die Einrichtung NUR in begründeten Einzelfallentscheidungen zulassen.

f) Die Einrichtung MUSS die Sicherheitsnachweise des Cloud-Diensteanbieters auswerten. Insbesondere DÜRFEN Prüfberichte und Nachweise über den Nutzungszeitraum KEINE zeitlichen Lücken enthalten.

g) Die Einrichtung MUSS sich die Einhaltung vorgesehener und vereinbarter Prozesse sowie die Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen durch den Cloud-Diensteanbieter vertraglich zusichern lassen.

h) Die Einrichtung MUSS ermittelte Risiken, die nicht bereits durch Basiskriterien nach C5 abgedeckt sind, über zusätzliche Anforderungen abdecken oder diese Risiken transferieren oder diese Risiken tragen.

---

[25] Hinweis: Liegt ein Prüfbericht nach C5 vor, können diese Informationen daraus entnommen werden.

[26] Hinweis: Der Auswertungsleitfaden gibt eine Struktur vor, welche die Einrichtung darin unterstützt, einen C5-Bericht systematisch auszuwerten. Dies beinhaltet, die Sicherheitsmaßnahmen des Cloud-Diensteanbieters (und die zugehörigen Prüfergebnisse) aufzunehmen, die eigenen Nutzerkontrollen für die Nutzung einzurichten und hierdurch das mit der Cloud-Nutzung verbundene Risiko einzuschätzen und steuern zu können. Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“, (BSI 2020c), https://www.bsi.bund.de

[27] Hinweis: Die im C5 festgelegten Übergangsfristen für neue Versionen sind zu beachten.

[28] Hinweis: Im Falle einer „direkten Prüfung“ (vgl. C5, (BSI 2020a), Kap. 4.4.5, S.16f.) enthält der Bericht keine Systembeschreibung vom Anbieter, sondern eine vom Prüfer im Rahmen der Prüfung erhobene Beschreibung mit vergleichbarem Inhalt, die im Rahmen der Tätigkeiten dieses Mindeststandards herangezogen werden kann.

i) Die Einrichtung MUSS prüfen, ob sie weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) unterliegt, die hinsichtlich der Cloud-Nutzung relevant sind. Diese Anforderungen MUSS die Einrichtung einhalten. Sie werden im Übrigen durch diesen Mindeststandard nicht berührt.

ii) Für die zusätzlichen Anforderungen MUSS die Einrichtung vereinbaren, dass regelmäßig geeignete Nachweise ihrer angemessenen und wirksamen Umsetzung vorgelegt werden.

i) Die Einrichtung SOLLTE sich eigene Prüfrechte vertraglich zusichern lassen.

i) Aufgrund der Ergebnisse aus der Datenkategorisierung und Risikoanalyse KANN die Einrichtung in begründeten Fällen auf eigene Prüfrechte verzichten, soweit Rechtsvorschriften nicht entgegenstehen.

ii) Die Einrichtung MUSS darauf achten, dass die Prüfrechte so ausgestaltet sind, dass die Einrichtung ihre gesetzlichen Anforderungen erfüllt.

iii) Die Einrichtung MUSS die Prüfrechte so ausgestalten, dass sie nach Art und Umfang einen Nachweis des Schutzniveaus ermöglichen und die Prüfung durch die Einrichtung selbst oder durch Dritte in ihrem Auftrag (z. B. andere Stellen, externe IT-Revisoren oder Wirtschaftsprüfer) durchgeführt werden kann.

iv) Sofern der Cloud-Diensteanbieter keinen Prüfbericht nach C5 vorlegen kann, MUSS die Einrichtung dazu berechtigt sein, die Prüfung nach C5 durch Dritte selbst beauftragen zu können.

### NCD.2.2.02 Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern

a) Die Einrichtung MUSS sich die Beteiligung von relevanten Unterauftragnehmern und anderen externen Dritten vom Cloud-Diensteanbieter vollständig in Art und Umfang benennen lassen. Die Entscheidung, welcher Unterauftragnehmer hier zu nennen ist, MUSS gemäß den Vorgaben des C5[29] erfolgen.

b) Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vereinbaren, dass beabsichtigte Änderungen hierüber unverzüglich schriftlich oder per E-Mail mitgeteilt werden.

c) Diese Mitteilungen KÖNNEN über Internetportale bereitgestellt werden, wenn dadurch die Anforderungen gleichwertig erfüllt sind (z. B. durch Push-Benachrichtigungen).

d) Falls Unterauftragnehmer wesentliche Teile[30] zur Entwicklung oder zum Betrieb des Cloud-Dienstes beitragen, MUSS sich die Einrichtung vom Cloud-Diensteanbieter zusichern lassen, dass

- Unterauftragnehmer ebenfalls die vertraglich festgelegten Vorgaben erfüllen und
- zugesicherte Prüfrechte sich auch auf Unterauftragnehmer beziehen.

### NCD.2.2.03 Gerichtsbarkeit vertraglich zusichern

a) Die Einrichtung SOLLTE zur Absicherung der Verfügbarkeit als Teil der Informationssicherheit Vereinbarungen ausschließlich nach deutschem Recht und deutschem Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren abschließen.

b) Die Einrichtung MUSS berücksichtigen, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtsschutz Zeitverluste eintreten können, insbesondere durch eine Einarbeitung in fremde Rechtsordnungen oder ein Auftreten vor entfernt gelegenen Gerichten.

c) Die Einrichtung MUSS sicherstellen, dass sie handlungsfähig bleibt und ihre Forderungen effektiv durchsetzen kann.

[29] Kriterienkatalog Cloud Computing (C5), (BSI 2020a), Kap. 4.4.5, S.18f.
[30] Hinweis: Hinsichtlich Bestimmung „wesentlicher Teile“ siehe C5, (BSI 2020a), S.91

#### NCD.2.2.04 Lokation vertraglich zusichern

a) Die Einrichtung MUSS sämtliche Lokationen, an denen dienstliche Daten verarbeitet werden, vertraglich festlegen.

b) Die Einrichtung MUSS prüfen, ob die dienstlichen Daten an den vertraglich zugesicherten Lokationen verarbeitet werden dürfen. Dabei MUSS die Einrichtung die Ergebnisse der Datenkategorisierung und Risikoanalyse sowie der möglichen Gefahr eines fremdstaatlichen Zugriffs (z. B. durch Nachrichtendienste oder Ermittlungsbehörden) bewerten.

#### NCD.2.2.05 Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern

a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter zusichern lassen, dass Daten nicht in den Bereich fremdstaatlicher Offenbarungspflichten und Ermittlungsbefugnisse gelangen.[31]

b) Die Einrichtung MUSS die Pflichten des Cloud-Diensteanbieters, sicherheitsrelevante Vorfälle (sowie ggf. andere Vorfälle) gegenüber der Einrichtung zu melden, vertraglich regeln.

i) Die Einrichtung MUSS bei Vertragsstrafen und Haftungsfragen auf ein angemessenes Verhältnis zum ermittelten Schutzbedarf achten.

ii) Bei der Festlegung sind die aus rechtlicher Sicht zulässigen Grenzen zu berücksichtigen. Die Einrichtung SOLLTE bei der Ansetzung von Vertragsstrafen 5% des Auftragsvolumens nicht unterschreiten.

#### NCD.2.2.06 Beendigung des Vertragsverhältnisses regeln

a) Die Einrichtung MUSS Kündigungsfristen dem Einsatzszenario angemessen festlegen.

b) Soweit rechtlich möglich, MUSS die Einrichtung kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte an den Leistungen zu Lasten der Einrichtung ausschließen.

#### NCD.2.2.07 Datenrückgabe und Datenlöschung beim Cloud-Diensteanbieter vertraglich zusichern

a) Die Einrichtung MUSS die Rückgabe der Daten regeln (Format, Datenträger, Protokolle, usw.).

b) Die Einrichtung MUSS berücksichtigen, dass die Maßnahmen zur Datenlöschung dem ermittelten Schutzbedarf entsprechen.

## 2.3 Einsatzphase

Mindestanforderungen an den Einsatz von externen Cloud-Diensten regeln, wie die vertraglich zugesicherten Leistungen überwacht und überprüft werden.

#### NCD.2.3.01 ISMS einbinden

a) Die Einrichtung MUSS den externen Cloud-Dienst in ihr eigenes Informationssicherheitsmanagementsystem (ISMS) einbinden.

b) Die Einrichtung MUSS die im C5-Bericht genannten korrespondierenden Kontrollen des Cloud-Dienstes bei sich einrichten. Die Einrichtung SOLLTE bei der Einbindung in das eigene ISMS zusätzlich die korrespondierenden Kriterien des C5[32] berücksichtigen.

#### NCD.2.3.02 Sicherheitsnachweise prüfen

[31] Auf die geltenden Regelungen zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden wird in diesem Zusammenhang entsprechend verwiesen. (BMI 2014), S.1

[32] Hinweis: Der C5 führt mit Version 2020 Mitwirkungspflichten des Kunden als korrespondierende Kriterien ein. Die Umsetzung liegt im Verantwortungsbereich des Kunden und ist entscheidend für die Aufrechterhaltung der Informationssicherheit eines Cloud-Dienstes. Siehe C5, (BSI 2020a), S.9

a) Die Einrichtung MUSS die Nachweise und sonstige Berichte des Cloud-Diensteanbieters auswerten.[33]

i) Diese DÜRFEN über den Nutzungszeitraum KEINE zeitlichen Lücken enthalten.

ii) Ergeben sich aus der Auswertung Unklarheiten, MUSS die Einrichtung diesen nachgehen.

b) Die Einrichtung MUSS prüfen, ob festgestellte Unklarheiten durch Wahrnehmung der zugesicherten Prüf- und Kontrollrechte nachzugehen ist.

**NCD.2.3.03 Leistungsfähigkeit prüfen**

a) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten ihrer eigenen IT-Infrastruktur, wie Performance der Netzanbindung und -verbindungen, beurteilen.

b) Die Einrichtung MUSS auf Abweichungen reagieren und die eigene IT-Infrastruktur und Netzanbindung den Ergebnissen der Überprüfung anpassen.

c) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten des Cloud-Diensteanbieter, wie Performance des Cloud-Services und die Netzverbindung zum Cloud-Diensteanbieter, beurteilen.[34]

**NCD.2.3.04 Informationspflichten nachhalten**

a) Die Einrichtung MUSS nachhalten, dass der Cloud-Diensteanbieter seinen vertraglichen Informationspflichten stets nachkommt. Dies gilt insbesondere bei

i) einer Eingliederung in ein anderes Unternehmen oder einen anderen Konzern oder in sonstigen Fällen des Wechsels des wirtschaftlichen Eigentums an ihn,

ii) einem Austausch von Unterauftragnehmern oder Dritten.

b) Die Einrichtung MUSS Meldungen des Cloud-Diensteanbieters über relevante Störungen und Cyber-Angriffe dokumentieren und gemäß den vereinbarten Mitwirkungspflichten nach NCD.2.2.01, Buchstabe c) reagieren.

**NCD.2.3.05 Zwei-Faktor-Authentifizierungen aktivieren**

a) Bietet der externe Cloud-Dienst eine Zwei-Faktor-Authentifizierung als Identitätsnachweis seiner Benutzer (Log-in) an, SOLLTE die Einrichtung diese nutzen.

## 2.4 Beendigungsphase

Mindestanforderungen an die Beendigung der Cloud-Nutzung adressieren die geordnete Beendigung des Vertragsverhältnisses.[35]

**NCD.2.4.01 Datenrückgabe durchführen**

a) Die Einrichtung MUSS prüfen, ob der Cloud-Diensteanbieter alle Daten in der vereinbarten Form zurück übergeben hat.

b) Die Einrichtung MUSS die Übergabe dokumentieren.

**NCD.2.4.02 Datenlöschung bestätigen**

a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter die Löschung aller Daten, einschließlich vorhandener Datensicherungen, bestätigen lassen.

b) Die Bestätigung nach Buchstabe a) MUSS auch Daten und Datensicherungen bei möglichen Unterauftragnehmern und anderen externen Dritten umfassen.

c) Die Einrichtung MUSS die Datenlöschung dokumentieren.

---

[33] Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“, (BSI 2020c), https://www.bsi.bund.de

[34] Hinweis: Viele Cloud-Diensteanbieter stellen diese Information kontinuierlich bereit, so dass diese Überprüfung als kontinuierliches Monitoring ausgestaltet werden kann. Mit dieser Anforderung ist gemeint, dass die vom Cloud-Diensteanbieter gelieferten oder von der Einrichtung erhobenen Daten zur Leistungsfähigkeit regelmäßig (mindestens jährlich) zu einer Beurteilung der Leistungsfähigkeit verdichtet und bewertet werden.

[35] Siehe OPS.2.2.A14 *Geordnete Beendigung eines Cloud-Nutzungsverhältnisses*, (BSI 2020b), S.1ff

## 2.5 Sicherheitsanforderungen bei einer Mitnutzung

Nehmen Benutzer einer Einrichtung einen externen Cloud-Dienst in Anspruch, ohne dass zwischen dieser Einrichtung und Cloud-Diensteanbieter ein Vertragsverhältnis besteht, geht dieser Mindeststandard von einer sog. Mitnutzung aus.[36] Für diesen Anwendungsfall regeln die nachfolgenden Sicherheitsanforderungen das Mindestsicherheitsniveau.

### NCD.2.5.01 Mitnutzung von externen Cloud-Diensten

a) Die Einrichtung MUSS die Sicherheitsanforderungen nach NCD.2.1.03, Buchstaben d) bis i) umsetzen und einhalten.

b) Die Einrichtung MUSS ermitteln, an welchen Lokationen dienstliche Daten verarbeitet werden.

i) Die Einrichtung MUSS dann bewerten, ob aus ihrer Sicht die dienstlichen Daten an diesen Lokationen verarbeitet werden dürfen.

ii) Für diese Bewertung MUSS die Einrichtung insbesondere die Ergebnisse der Datenkategorisierung heranziehen.

c) Die Einrichtung MUSS ermitteln, welche Rechte dem Cloud-Diensteanbieter oder Dritten an den dienstlichen Daten eingeräumt werden.

i) Die Einrichtung MUSS bewerten, ob diese Rechte mit der eigenen Sicherheitsrichtlinie vereinbar sind.

ii) Die Einrichtung MUSS insbesondere die Nutzungsbedingungen und die Datenschutzerklärung des Cloud-Diensteanbieters auswerten.

d) Die Einrichtung MUSS ermitteln, wie die dienstlichen Daten im externen Cloud-Dienst verschlüsselt gespeichert werden.

i) Die Einrichtung MUSS dann bewerten, ob die Verschlüsselung mit den Anforderungen aus den Ergebnissen der Datenkategorisierung vereinbar sind.

ii) Ist die vom Cloud-Diensteanbieter eingesetzte Verschlüsselung nicht geeignet, MUSS die Einrichtung prüfen, ob Anforderungen an die Vertraulichkeit der Daten über eine clientseitige Verschlüsselung erfüllt werden können.

e) Die Einrichtung MUSS ermitteln, ob für die Mitnutzung auf den eigenen Arbeitsplatzcomputern oder mobilen Endgeräten zusätzliche Softwareinstallationen erforderlich sind.

i) Die Einrichtung MUSS dann bewerten, ob die hierfür einzuräumenden Zugriffs- und Ausführungsrechte mit der eigenen IT-Sicherheitsrichtlinie vereinbar sind und inwiefern gesonderte Lizenzen für die Mitnutzung eingeholt werden müssen.

ii) Ist ein Zugriff über mobile Endgeräte geplant, MUSS die Einrichtung diese zentral verwalten. Die Vorgaben des Mindeststandards Mobile Device Management sind zu beachten.[37]

[36] Hinweis: Ein Akzeptieren von Allgemeinen Geschäftsbedingungen (AGB) oder sonstigen Nutzungsbedingungen sind nicht als ein Vertragsverhältnis im Sinne dieses Mindeststands anzusehen.
[37] Siehe Mindeststandard des BSI Mobile Device Management, (BSI 2017), S.1ff.

# Literaturverzeichnis


AKTM (2011) Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, Orientierungshilfe – Cloud Computing, Version 2.0, Oktober 2014

BMI (2014) Bundesministerium des Innern, Erlass zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden, O4 - 11032/23#14, Berlin 2014

BMI (2017) Bundesministerium des Innern, für Bau und Heimat: Umsetzungsplan Bund 2017 – Leitlinie für die Informationssicherheit in der Bundesverwaltung

BMI (2018) Bundesministerium des Innern, für Bau und Heimat: Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), 10. August 2018

BSI (2008) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-4 – Notfallmanagement, Version 1.0

BSI (2017a) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-2 – IT-Grundschutz-Methodik, Version 1.0

BSI (2017b) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI für Mobile Device Management, Version 1.0

BSI (2019) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandards – Antworten auf häufig gestellte Fragen zu den Mindeststandards, https://www.bsi.bund.de/dok/11916758, abgerufen am 17.11.2020

BSI (2020a) Bundesamt für Sicherheit in der Informationstechnik: Kriterienkatalog Cloud Computing, Version 1.0 – Stand Februar 2020

BSI (2020b) Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, 3. Edition 2020

BSI (2020c) Bundesamt für Sicherheit in der Informationstechnik: Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5, https://www.bsi.bund.de/dok/14020574, abgerufen am 17.11.2020

DIN (2018) Deutsches Institut für Normierung e.V.: Normungsarbeit – Teil 2: Gestaltung von Dokumenten, DIN 820-2:2018-09

IETF (1997) Internet Engineering Task Force: Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, https://tools.ietf.org/html/rfc2119, abgerufen am 17.11.2020

# Abkürzungsverzeichnis

| | |
|---|---|
| AGB | Allgemeine Geschäftsbedingungen |
| BMI | Bundesministerium des Innern, für Bau und Heimat |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| BSIG | Gesetz über das Bundesamt für Sicherheit in der Informationstechnik |
| BDSG | Bundesdatenschutzgesetz |
| C5 | Kriterienkatalog Cloud Computing |
| DIN | Deutsches Institut für Normierung e.V. |
| FAQ | Frequently Asked Questions |
| IETF | Internet Engineering Task Force |
| ISB | Informationssicherheitsbeauftragte |
| ISMS | Informationssicherheitsmanagementsystem |
| IT-SiBe | IT-Sicherheitsbeauftragte |
| StGB | Strafgesetzbuch |
| RFC | Request for Comments |
| VSA | Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA) |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise |
|---|---|---|
| **1 Beschreibung** | **1 Beschreibung** | |
| Dieser Mindeststandard definiert Sicherheitsanforderungen an die Nutzung externer Cloud-Dienste. | Dieser Mindeststandard setzt Sicherheitsanforderungen an die Nutzung externer Cloud-Dienste. | |
| Diese Anforderungen sind einzuhalten, um ein Mindestmaß an Informationssicherheit beim Nutzen derartiger Dienste zu gewährleisten. | Die Erfüllung der im Mindeststandard vorgegebenen Sicherheitsanforderungen ist für ein angemessenes IT-Sicherheitsniveau notwendig, aber in der Regel nicht hinreichend.<br>Unter Berücksichtigung des individuellen Schutzbedarfs muss die Festlegung und Umsetzung eventuell zusätzlich erforderlicher Sicherheitsanforderungen erfolgen. | |
| Er richtet sich hinsichtlich seiner Umsetzung an IT-Verantwortliche, IT-Sicherheitsbeauftragte[xx] und IT-Fachkräfte sowie mit der Beschaffung beauftragte Stellen.<br><br>[xx] Bzw. Informationssicherheitsbeauftragte | Er richtet sich hinsichtlich seiner Umsetzung an IT-Sicherheitsbeauftragte, IT-Betriebs- und Fachverantwortliche.[xx]<br><br>[xx] Rollen nach IT-Grundschutz-Kompendium, (BSI 2020b), S.1ff. | I. Wording IT-Grundschutz-Kompendium. Hier Rollen<br>II. Fußnote zu „Informationssicherheitsbeauftragter“ entfallen, jetzt im Vorwort<br>III. Fußnote Rollen nach IT-GS eingefügt. |
| Anbieter von Cloud-Diensten und andere interessierte Personen können diesen Mindeststandard zur Erhöhung der Informationssicherheit oder zum Abgleich ihrer Angebote heranziehen. | | I. Satz gestrichen, kein Regelungsinhalt. Gilt generell und wird auf der BSI-Webseite entsprechend klargestellt. |
| | **1.1 Begriffsbestimmung und Abgrenzung** | I. Unterkapitel zur besseren Strukturierung eingeführt |
| Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Insbesondere werden dabei Infrastrukturen, Plattformen und Software angeboten, die Spannbreite der angebotenen Cloud-Dienste umfasst darüber hinaus jedoch das komplette Spektrum der Informationstechnik.[xx]<br>[xx] BSI (2017), https://www.bsi.bund.de/cloud External Link | Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Insbesondere werden dabei Infrastrukturen, Plattformen und Software angeboten, die Spannbreite der angebotenen Cloud-Dienste umfasst darüber hinaus jedoch das komplette Spektrum der Informationstechnik.[xx]<br>[xx] Definition nach https://www.bsi.bund.de/cloud | |
| Externe Cloud-Dienste im Sinne dieses Mindeststandards sind im Rahmen von Cloud Computing angebotene Dienstleistungen, die über Netzwerke und Anbieter der Wirtschaft außerha b der öffentlichen Verwaltung des Bundes und der Länder erbracht werden. | Externe Cloud-Dienste im Sinne dieses Mindeststandards sind im Rahmen von Cloud Computing angebotene Dienstleistungen, die über Netze und Anbieter der Wirtschaft außerhalb der öffentlichen Verwaltung des Bundes und der Länder erbracht werden.[xx]<br>[xy] Hinweis: IT-Dienstleistungen der „Bundescloud“ fallen somit nicht unter diese Bestimmung. | I. Fußnote „Bundescloud“ eingefügt |
| Als Nutzung ist insbesondere die Beauftragung eines externen Cloud-Dienstes durch eine Stelle des Bundes selbst oder gemeinsam mit anderen zu verstehen. | Als Nutzung ist eine Verarbeitung von dienstlichen Daten[xx] durch einen externen Cloud-Dienst zu verstehen, der durch die Einrichtung se bst oder gemeinsam mit anderen beauftragt wird. | I. Nutzungsbegriff auf „dienstliche Daten“ konkretisiert<br>II. Fußnote „dienstliche Daten“ hinzugefügt. |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise |
|---|---|---|
| | [xx] Dienstlich sind alle Daten, die im Rahmen der dienstlichen Tätigkeit erhoben und verarbeitet werden. Darunter fallen jedoch nicht personenbezogene Daten (wie Stammdaten, Nutzungsdaten), die für die Registrierung und Nutzung des Dienstes vom Cloud-Diensteanbieter erhoben oder verarbeitet werden. | |
| | Werden externe Cloud-Dienste durch Benutzer[xx] einer Einrichtung lediglich mitgenutzt, regelt Kapitel 2.5 den Umgang mit dienstlichen Daten in diesen Fällen entsprechend. Von einer Mitnutzung wird insbesondere ausgegangen, wenn die Einrichtung den externen Cloud-Diensten nicht beauftragt hat.<br>xx Analog Rolle „Benutzer" nach IT-Grundschutz-Kompendium, (BSI 2020b), S.31 | **Hinweis:**<br>Aufnahme zur Mitnutzung (siehe Kapitel 2.5) |
| | Werden keine dienstlichen Daten verarbeitet, können die Regelungen des Mindeststandards trotzdem angewendet werden (siehe NCD.2.1.03, Buchstabe e)). | I. Satz neu hinzugefügt. |
| | **1.2 Modalverben** | **Hinweis:** Einführung von Modalverben<br>Einheitlicher und abgestimmter Text. Bitte im Kapitel 1.2 keine Änderungen vornehmen! |
| Dieser Mindeststandard setzt die IT-Grundschutz-Vorgehensweise des BSI zum Management der Informationssicherheit voraus.[xx]<br>xx Vgl. BSI (2008), S.49f. | In Anlehnung an den IT-Grundschutz[xx] werden die Anforderungen mit den Modalverben „MUSS" und „SOLLTE" sowie den zugehörigen Verneinungen formuliert. Darüber hinaus wird das Modalverb KANN für ausgewählte Prüfaspekte verwendet.<br>[xx] Vgl. BSI-Standard 200-2, (BSI 2017), S.18 | |
| Er gilt für alle Schutzbedarfskategorien. | Die hier genutzte Definition basiert auf RFC 2119[xx] und DIN 820-2: 2018[xy].<br>[xx] Vgl. Key words for use in RFCs to Indicate Requirement Levels, (IETF 1997)<br>[xy] Vgl. Normungsarbeit – Teil 2: Gestaltung von Dokumenten, (DIN 2018) | |
| | **MUSS / DARF NUR**<br>bedeutet, dass diese Anforderung zwingend zu erfüllen ist. Das von der Nichtumsetzung ausgehende Ris ko kann nicht im Rahmen einer Risikoanalyse akzeptiert werden. | |
| | **DARF NICHT / DARF KEIN**<br>bedeutet, dass etwas zwingend zu unterlassen ist. Das durch die Umsetzung entstehende Risiko kann nicht im Rahmen einer Risikoanalyse akzeptiert werden. | |
| | **SOLLTE**<br>bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können. | |
| | **SOLLTE NICHT / SOLLTE KEIN**<br>bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können. | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise |
|---|---|---|
| | **KANN**<br>bedeutet, dass die Umsetzung / Nicht-Umsetzung optional ist und ohne Angabe von Gründen unterbleiben kann. | |
| **2 Sicherheitsanforderungen** | **2 Sicherheitsanforderungen** | **Hinweis:** Die Reihenfolge der Sicherheitsanforderungen hat sich gegenüber der V1.0 geändert.<br>Um diese dennoch leicht vergleichen zu können, sind die Anforderungen aus der V1.0 den Anforderungen aus V1.0.5 thematisch zugeordnet. |
| Nachfolgende Sicherheitsanforderungen adressieren die Beschaffungs- (Kapitel 2.1), die Einsatz- (Kapitel 2.2) sowie die Beendigungsphase (Kapitel 2.3) von externen Cloud-Diensten. Diese sind einzuhalten, um ein Mindestmaß an Informationssicherheit zu gewährleisten. Sie können jedoch bei Bedarf durch zusätzliche Anforderungen erweitert werden. | Nachfolgende Sicherheitsanforderungen adressieren die Informationssicherheit entlang des gesamten Lebenszyklus und setzen auf den IT-Grundschutz-Baustein OPS.2.2 *Cloud-Nutzung*[xx] auf.<br>[xx] IT-Grundschutz-Kompendium, (BSI 2020b), OPS.2.2: *Cloud-Nutzung* | I. Einbindung des IT-Grundschutz-Bausteins OPS.2.2.<br>II. Text gekürzt. |
| | **2.1. Planungsphase** | I. Planungsphase zur besseren Strukturierung eingeführt.<br>Hinweis: Bisher waren diese Regelungen als Erklärungstext implementiert. Diese sind jetzt als konkrete Anforderungen gesetzt! |
| Vor der Nutzung externer Cloud-Dienste ist zusätzlich zur Schutzbedarfsfeststellung aus dem IT-Grundschutz eine vorgelagerte Datenkategorisierung und Risikoanalyse durchzuführen. | Grundlage der Informationssicherheit im Bereich Cloud Computing bilden nach dem IT-Grundschutz-Baustein OPS2.2 *Cloud-Nutzung*<br>– die Cloud-Nutzungs-Strategie<br>– die darauf basierende Sicherheitsrichtlinie sowie<br>– das jeweilige Sicherheitskonzept für den externen Cloud-Dienst.<br>Die nachfolgenden Sicherheitsanforderungen adressieren diese Dokumente entsprechend. | I. Bezug auf IT-GS, hier Cloud-Nutzungs-Strategie der Einrichtung, Sicherheitsrichtlinie und Sicherheitskonzept. |
| | **NCD.2.1.01 Cloud-Nutzungs-Strategie** | **Hinweis:** OPS.2.2 fordert die Erstellung einer Cloud-Nutzungs-Strategie. Auf diese wird in der Sicherheitsanforderung verwiesen bzw. diese wird inhaltlich konkretisiert. |
| | a) Die Einrichtung MUSS prüfen, ob der externe Cloud-Dienst grundsätzlich mit den in der Cloud-Nutzungs-Strategie definierten Zielen, Chancen und Risiken vereinbar ist.[xx]<br>[xx] Hinweis: OPS.2.2.A1 Erstellung einer Cloud-Nutzungs-Strategie sieht die Erstellung einer Cloud-Nutzungs-Strategie vor. In dieser erfasst die Einrichtung ihre Ziele, Chancen und Risiken, die sie mit einer Cloud-Nutzung generell verbindet. Die Cloud-Nutzungs-Strategie nimmt daher eine zentrale Rolle für die Einrichtung ein. | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise |
|---|---|---|
| | Sie wird benötigt, um die beabsichtigte Nutzung eines konkreten externen Cloud-Dienstes bewerten zu können. | |
| | b) Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn Ziele, Chancen und Ris ken der Cloud-Nutzungs-Strategie angemessen berücksichtigt werden können. | |
| | **NCD.2.1.02: Sicherheitsrichtlinie externe Cloud-Dienste** | **Hinweis**: OPS.2.2 fordert die Erstellung einer Sicherheitsrichtlinie. Auf diese wird in der Sicherheitsanforderung verwiesen bzw. diese wird inhaltlich konkretisiert. |
| | a) Die Einrichtung MUSS eine Sicherheitsrichtlinie für externe Cloud-Dienste nach OPS.2.2.A2 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*[xx] erstellen.<br>[xx] IT-Grundschutz-Kompendium, (BSI 2020b), OPS.2.2: *Cloud-Nutzung* | **Hinweis:** War vorher in „CD.01: Systembeschreibung und weitergehende Informationen fordern" enthalten!<br>(siehe weiter unten) |
| | b) Die Einrichtung MUSS in dieser Sicherheitsrichtlinie mindestens die Umsetzung und Einhaltung der Basiskriterien nach dem Kriterienkatalog Cloud Computing (C5) als spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter festlegen.[xx]<br>[xx] Kriterienkatalog Cloud Computing (C5), (BSI 2020a), S.1ff. | I. hier werden jetzt die Basiskriterien des C5 verankert. Vorher war dies in der Leistungsbeschreibung. |
| | c) Die Einrichtung MUSS die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragen bei der Erstellung der Sicherheitsrichtlinie beteiligen. | I. Beteiligung war vorher auf Risikoanalyse und Datenkategorisierung beschränkt! |
| | **NCD.2.1.03: Sicherheitskonzept für den externen Cloud-Dienst** | |
| | a) Die Einrichtung MUSS ein Sicherheitskonzept für den externen Cloud-Dienst nach OPS.2.2.A7 *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung* erstellen. | **Hinweis:** OPS.2.2 fordert die Erstellung eines Sicherheitskonzeptes. Auf dieses wird in der Sicherheitsanforderung verwiesen bzw. das Siko wird inhaltlich konkretisiert. |
| Die Risikoanalyse ist insbesondere vor dem Hintergrund aktueller Veröffentlichungen des BSI zu Cloud-Sicherheit vorzunehmen.[xx]<br>[xx] Siehe hierzu insbesondere „Anforderungskatalog Cloud Computing des BSI" (Cloud Computing Compliance Controls Catalogue, kurz C5). | b) Die Einrichtung MUSS in dem Sicherheitskonzept die aktuellen Veröffentlichungen des BSI zu Cloud-Sicherheit berücksichtigen.[xx]<br>[xx] siehe Veröffentlichungen unter https://www.bsi.bund.de/cloud | |
| Im Rahmen dieser Risikoanalyse sind die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragen zu beteiligen. | c) Die Einrichtung MUSS die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragen bei der Erstellung des Sicherheitskonzeptes beteiligen. | I. jetzt Beteiligung bei Sicherheitskonzept, dies schließt dann Risikoanalyse und Datenkategorisierung mit ein! |
| | d) Die Einrichtung MUSS eine Datenkategorisierung durchführen, in der sämtliche dienstliche Daten identifiziert werden, die künftig in dem externen Cloud-Dienst verarbeitet werden sollen. | I. Feststellung, ob überhaupt dienstliche Daten verarbeitet werden sollen! |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise |
|---|---|---|
| | e) Kommt die Einrichtung zu dem Ergebnis, dass in dem externen Cloud-Dienst keine dienstlichen Daten verarbeitet werden, handelt es sich nicht um eine Nutzung oder Mitnutzung externer Cloud-Dienste im Sinne dieses Mindeststandards. In diesem Fällen KANN die Einrichtung die Sicherheitsanforderungen des Mindeststandards umsetzen. | I. Klarstellung, wann MST-Regelungen Anwendung finden! |
| In der Datenkategorisierung sind zusätzlich zum Schutzbedarf Geheim- und Datenschutzaspekte[xx] sowie Personen- und Dienstgeheimnisse zu ermitteln.<br>[xx] Hinsichtlich Datenschutzaspekte siehe insbesondere AKTM (2011), S.1ff. | f) Die Einrichtung MUSS für die identifizierten dienstlichen Daten Geheim- und Datenschutzaspekte[xx] sowie Personen- und Dienstgeheimnisse ermitteln.<br>[xx] Hinsichtlich Datenschutzaspekte siehe insbesondere (AKTM 2011), S.1ff. | |
| Im Rahmen der Datenkategorisierung sind die Daten den nachfolgenden Kategorien zuzuordnen:<br>– Kategorie 1 = Privat- und Dienstgeheimnisse gemäß §§ 203 und 353b StGB<br>– Kategorie 2 = personenbezogene Daten gemäß § 3 Absatz 1 BDSG<br>– Kategorie 3 = Verschlusssachen gemäß allgemeiner Verwaltungsvorschrift des BMI zum materiellen und organisatorischen Schutz von Verschlusssachen (VSA)<br>– Kategorie 4 = sonstige Daten (weder Kategorie 1, noch 2, noch 3)<br>Daten können den Kategorien 1, 2 oder 3 gleichzeitig angehören. Die Kategorisierung der Daten ist zu dokumentieren. | g) Die Einrichtung MUSS die identifizierten dienstlichen Daten den nachfolgenden Kategorien zuordnen:<br>– Kategorie 1 = Privat- und Dienstgeheimnisse gemäß §§ 203 und 353b StGB<br>– Kategorie 2 = personenbezogene Daten gemäß § 3 Absatz 1 BDSG<br>– Kategorie 3 = Verschlusssachen gemäß Verschlusssachenanweisung - VSA[xx]<br>– Kategorie 4 = sonstige Daten (weder Kategorie 1, noch 2, noch 3)<br>h) Die Einrichtung KANN die identifizierten dienstlichen Daten den Kategorien 1, 2 oder 3 gleichzeitig zuordnen.<br>[xx] Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA), (BMI 2018) | |
| | i) Die Einrichtung MUSS Risiken, die aus der künftigen Nutzung des externen Cloud-Dienstes entstehen können, umfassend ermitteln.[xx]<br>[xx] Hinweis: Bei dieser Prüfung geht es um eine anbieterunabhängige Prüfung. Es soll in diesem Zusammenhang geklärt werden, ob das beabsichtigte Cloud-Szenario mit der Cloud-Nutzung-Strategie vereinbar ist (z.B. Können die eigenen rechtlichen und organisatorischen Rahmenbedingungen überhaupt erfüllt werden?) | |
| Die ermittelten Ris ken für die Daten müssen betrachtet und bewertet werden. | i) Die Einrichtung MUSS die ermittelten Ris ken mit denen in der eigenen Cloud-Nutzungs-Strategie (siehe NCD.2.1.01) festgelegten Richtlinien der Ris kobewertung abgleichen und bewerten. | |
| | ii) Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn die ermittelten Risiken gemäß der in der Cloud-Nutzungs-Strategie genannten Richtlinien zur Risikobewertung, wirksam vermieden oder hinreichend reduziert oder getragen werden können. | |
| Auch auf Seiten der Stelle des Bundes können je nach Nutzungsszenario in allen Phasen der Cloud-Nutzung zusätzliche Maßnahmen erforderlich sein. | | **Hinweis:** keine Anforderung, sondern nur als Hinweistext. Wurde daher nicht übernommen |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise |
|---|---|---|
| | **NCD.2.1.04: Notfall- und Kontinuitätsmanagement** | **Hinweis:**<br>Anforderung neu hinzugefügt |
| | Mit Notfall- bzw. Kontinuitätsmanagement ist gemäß BSI-Standard 100-4[xx] ein Managementsystem zur Aufrechterhaltung einer definierten Arbeitsfähigkeit einer Einrichtung gemeint und umfasst sowohl präventive als auch reaktive Maßnahmen auf Notfälle und Krisensituationen. Es gilt im weiteren die Begrifflichkeit des BSI-Standards 100-4[xy].<br>[xx] BSI-Standard 100-4 – Notfallmanagement, (BSI 2008), S.1ff.<br>[xy] BSI-Standard 100-4 – Notfallmanagement, (BSI 2008), S.1ff. | **Hinweis:**<br>Nach Veröffentlichung von BSI 200-4 wird hier entsprechend angepasst. |
| | a) Die Einrichtung MUSS prüfen, ob sie in Notfällen und Krisensituationen weiter auf den externen Cloud-Dienst zugreifen können muss.[xx]<br>[xx] Hinweis: Leitfragen für diese Prüfung können sein: Wird der Cloud-Dienst für einen, im Notfallmanagement als zeitkrisitsch bewerteten Geschäftsprozess (bzw. Fachaufgabe) genutzt? Dient der Cloud-Dienst zur Etablierung und Aufrechterhaltung eines Notbetriebs? Ist der Cloud-Dienst für die Bewältigung eines Notfalles relevant? | |
| | b) Die Einrichtung MUSS bewerten, welche Bedeutung der externe Cloud-Dienst in Notfällen einnehmen würde.[xx]<br>xx Hinweis: Leitfragen für diese Prüfung können sein: Wie zeitkritisch sind die Geschäftsprozesse (bzw. Fachaufgaben), die den Cloud-Dienst in einem Notfall oder einer Krise benötigen? Zu welchem Grad wird der Cloud-Dienst in einem Notbetrieb benötigt? | |
| | c) Die Einrichtung MUSS den zuständigen Notfallbeauftragten entsprechend einbinden. Dieser MUSS prüfen, ob die Prävention vor bzw. die Reaktion auf Notfälle oder Krisen durch die Cloud-Nutzung geändert werden muss. Die Einrichtung MUSS diese Änderungen vor der Cloud-Nutzung umsetzen. | |
| **2.1 Beschaffungsphase** | **2.2 Beschaffungsphase** | |
| Ziel des Beschaffungsprozesses, für den die Vorgaben des Vergaberechts einschlägig sind, ist die Auswahl eines geeigneten Cloud-Anbieters. | Ziel des Beschaffungsprozesses, für den die Vorgaben des Vergaberechts einschlägig sind, ist die Auswahl eines geeigneten Cloud-Diensteanbieters. | I. Wording IT-GS (OPS.2.2 "Cloud-Nutzung"): Cloud-Anbieter durch Cloud-Diensteanbieter ersetzt. (Gilt für gesamte Dokument) |
| **2.1.1 Auswahl Cloud-Anbieter** | | Unterkapitel entfallen |
| Im Rahmen des Beschaffungsprozesses muss vom Bieter die Vorlage von Systembeschreibungen[xx], Zertifizierungen sowie Prüfberichten und anderen Nachweisen gefordert werden. Bei einer vorliegenden Testierung nach C5[xy] können die nachfolgend | | I. Einleitungstext entfallen, siehe Anforderung NCD.2.2.01, Buchstabe c) |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise |
|---|---|---|
| genannten Informationen aus der im Prüfbericht enthaltenen Systembeschreibung entnommen werden.<br>xx Beschreibung des Cloud-Dienste betreffenden internen Kontrollsystems (Systembeschreibung).<br>xy Vgl. BSI (2016), S.1ff. | | |
| **CD.01: Systembeschreibung und weitergehende Informationen fordern** | **NCD.2.2.0.1: Umsetzung der Sicherheitsanforderungen** | **Hinweis:** Anforderungen zusammengefasst. |
| | a) Die Einrichtung MUSS vor Vertragsabschluss überprüfen, ob die in ihrer Sicherheitsrichtlinie festgelegten Sicherheitsanforderungen (siehe NCD.2.1.02, Buchstabe a)) vom Cloud-Diensteanbieter erfüllt werden können.[xx]<br><br>[xx] Hinweis: Liegt ein Prüfbericht nach C5 vor, können diese Informationen daraus entnommen werden. | I. Konkretisierung auf die jeweilige Sicherheitsrichtlinie der Einrichtung<br>II. Hinweis auf Fundort in Fußnote. |
| Die Vorlage der Systembeschreibung des Cloud-Dienstes muss in der Leistungsbeschreibung gefordert werden. | b) Die Einrichtung MUSS diese Sicherheitsanforderungen bereits in der Leistungsbeschreibung des externen Cloud-Dienstes einfordern. | |
| Zur Beurteilung des Cloud-Anbieters können weitergehende Informationen im Rahmen der Leistungsbeschreibung gefordert werden.<br>Zudem sind mit Hilfe der Leistungsbeschreibung Basis- und Zusatzleistungen festzulegen. | | |
| Sie muss die Vorgaben nach C5 erfüllen und ist insbesondere auf Mitwirkungspflichten und Maßnahmen hin zu prüfen. | | **Hinweis:** Die Festlegung auf die Kriterien des C5 erfolgt bereits in Anforderung NCD.2.2.01; Mitwirkungspflichten und Maßnahmen jetzt in Buchstabe c) |
| **CD.03: Systembeschreibung und weitergehende Informationen auswerten**<br>Die Systembeschreibung und die weitergehenden Informationen müssen hinsichtlich Inhalt, Aussagekraft, Nachvollziehbarkeit, Aktualität und nachteiliger Regelungen ausgewertet werden.<br>Die Leistungsbeschreibung muss bereits genau definieren, welche Angaben vom Bieter erwartet werden.<br>Sofern die durch den Bieter vorgelegten Unterlagen Unklarheiten enthalten, muss geprüft werden, ob diese im Rahmen der Aufklärung aufzulösen sind oder zu Lasten des Bieters gehen. | c) Die Einrichtung MUSS die Angaben und Nachweise des Cloud-Diensteanbieters zu Buchstabe a) hinsichtlich Inhalt, Aussagekraft, Nachvollziehbarkeit, Aktualität, nachteiliger Regelungen sowie Mitwirkungspflichten und Maßnahmen auswerten. Dazu SOLLTE der „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“[xx] verwendet werden.<br>[xx] Hinweis: Der Auswertungsleitfaden gibt eine Struktur vor, welche die Einrichtung darin unterstützt, einen C5-Bericht systematisch auszuwerten. Dies beinhaltet, die Sicherheitsmaßnahmen des Cloud-Diensteanbieters (und die zugehörigen Prüfergebnisse) aufzunehmen, die eigenen Nutzerkontrollen für die Nutzung einzurichten und hierdurch das mit der Cloud-Nutzung verbundene Risiko einzuschätzen und steuern zu können. Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“, (BSI 2020c), https://www.bsi.bund.de | **Hinweis:**<br>I. Anforderungstext gekürzt.<br><br>II. Auswerteleitfaden hinzugefügt |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise |
|---|---|---|
| **CD.04: Sicherheitsnachweise vertraglich zusichern**<br>Der Cloud-Anbieter muss regelmäßig Sicherheitsnachweise über<br>– die angemessene und wirksame Umsetzung der Basisanforderungen nach C5,<br>– die aktuelle Dokumentation der Systembeschreibung,<br>– die Aktualität von vertraglich zugesicherten Zertifizierungen sowie<br>– die ordnungsgemäße Durchführung von Datensicherungen und erprobten Rücksicherungen<br>vorlegen.<br>Diese Sicherheitsnachweise sollten durch die regelmäßige Bereitstellung des aktuellen Prüfberichtes nach C5 erbracht werden. Andere Nachweise bedürfen der begründeten Einzelfallentscheidung. | d) Die Einrichtung MUSS sich die regelmäßige Vorlage von Sicherheitsnachweisen vom Cloud-Diensteanbieter zusichern lassen. | |
| | e) Diese Sicherheitsnachweise SOLLTEN<br>– die angemessene und wirksame Umsetzung der Basiskriterien nach C5[xx],<br>– die aktuelle Dokumentation der Systembeschre bung,[xy]<br>– die Aktualität von vertraglich zugesicherten Zertifizierungen sowie<br>– die ordnungsgemäße Durchführung von Datensicherungen und erprobten Rücksicherungen<br>umfassen und durch die regelmäßige Bereitstellung des aktuellen Prüfberichtes nach C5 erbracht werden. Andere Nachweise DARF die Einrichtung NUR in begründeten Einzelfallentscheidungen zulassen.<br>[xx] Hinweis: Die im C5 festgelegten Übergangsfristen für neue Versionen sind zu beachten.<br>[xy] Hinweis: Im Falle einer „direkten Prüfung" (vgl. C5, (BSI 2020), Kap. 4.4.5, S.16f.) enthält der Bericht keine Systembeschreibung vom Anbieter, sondern eine vom Prüfer im Rahmen der Prüfung erhobenen Beschreibung mit vergleichbarem Inhalt, die im Rahmen der Tätigkeiten dieses Mindeststandards herangezogen werden kann. | **Hinweis:**<br>I. Hinweis zur direkten Prüfung als Fußnote xy |
| Prüfberichte und Nachweise dürfen über den Nutzungszeitraum keine zeitlichen Lücken enthalten. | f) Die Einrichtung MUSS die Sicherheitsnachweise des Cloud-Diensteanbieters auswerten. Insbesondere DÜRFEN Prüfberichte und Nachweise über den Nutzungszeitraum KEINE zeitlichen Lücken enthalten. | |
| Die Einhaltung vorgesehener und vereinbarter Prozesse sowie die Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen durch den Cloud-Anbieter ist vertraglich zuzusichern. | g) Die Einrichtung MUSS sich die Einhaltung vorgesehener und vereinbarter Prozesse sowie die Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen durch den Cloud-Diensteanbieter vertraglich zusichern lassen. | |
| **CD.05: Zusätzliche Anforderungen vertraglich zusichern**<br>Ermittelte Gefährdungen bzw. Risiken, die nicht bereits durch Basisanforderungen nach C5 abgedeckt sind, müssen über zusätzliche Anforderungen abgedeckt werden.<br>Für die zusätzlichen Anforderungen ist zu vereinbaren, dass regelmäßig geeignete Nachweise ihrer angemessenen und wirksamen Umsetzung vorgelegt werden.<br>Die Stelle des Bundes hat zu prüfen, ob sie weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) unterliegt, die hinsichtlich der Cloud-Nutzung relevant sind. Diese Anforderungen sind einzuhalten und werden im Übrigen durch diesen Mindeststandard nicht berührt. | h) Die Einrichtung MUSS ermittelte Risiken, die nicht bereits durch die Basiskriterien nach C5 abgedeckt sind, über zusätzliche Anforderungen abdecken oder diese Risiken transferieren oder diese Ris ken tragen.<br>i) Die Einrichtung MUSS prüfen, ob sie weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) unterliegt, die hinsichtlich der Cloud-Nutzung relevant sind. Diese Anforderungen MUSS die Einrichtung einhalten. Sie werden im Übrigen durch diesen Mindeststandard nicht berührt.<br>ii) Für die zusätzlichen Anforderungen MUSS die Einrichtung vereinbaren, dass regelmäßig geeignete Nachweise ihrer angemessenen und wirksamen Umsetzung vorgelegt werden. | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise |
|---|---|---|
| **CD.06: Recht auf Prüfungen und Kontrollen vertraglich zusichern**<br>Grundsätzlich müssen der Stelle des Bundes eigene Prüfrechte vertraglich zugesichert werden.<br>Im Übrigen sind die Prüfrechte so auszugestalten, dass sie nach Art und Umfang einen Nachweis des Schutzniveaus ermöglichen und die Prüfung durch die Stelle des Bundes selbst oder durch Dritte in ihrem Auftrag (z. B. andere Stellen, externe IT-Revisoren oder Wirtschaftsprüfer) durchgeführt werden kann.<br>Aufgrund der Ergebnisse aus der Datenkategorisierung und Risikoanalyse kann in begründeten Ausnahmefällen auf eigene Prüfrechte verzichtet werden, soweit Rechtsvorschriften nicht entgegenstehen. Diese Entscheidung ist unter Risikogesichtspunkten zu treffen und zu dokumentieren.<br>Sofern der Cloud-Anbieter keinen Prüfbericht nach C5 vorlegen kann, muss die Stelle des Bundes dazu berechtigt sein, die Prüfung nach C5 durch Dritte se bst beauftragen zu können. | I) Die Einrichtung SOLLTE sich eigene Prüfrechte vertraglich zusichern lassen.<br>i) Aufgrund der Ergebnisse aus der Datenkategorisierung und Ris koanalyse KANN die Einrichtung in begründeten Fällen auf eigene Prüfrechte verzichten, soweit Rechtsvorschriften nicht entgegenstehen.<br>ii) Die Einrichtung MUSS darauf achten, dass die Prüfrechte so ausgestaltet sind, dass die Einrichtung ihre gesetzlichen Anforderungen erfüllt.<br>iii) Die Einrichtung MUSS die Prüfrechte so ausgestalten, dass sie nach Art und Umfang einen Nachweis des Schutzniveaus ermöglichen und die Prüfung durch die Einrichtung selbst oder durch Dritte in ihrem Auftrag (z. B. andere Stellen, externe IT-Revisoren oder Wirtschaftsprüfer) durchgeführt werden kann.<br>iv) Sofern der Cloud-Diensteanbieter keinen Prüfbericht nach C5 vorlegen kann, MUSS die Einrichtung dazu berechtigt sein, die Prüfung nach C5 durch Dritte selbst beauftragen zu können. | |
| **CD.02: Zertifizierungen oder Bescheinigungen unabhängiger Dritter festlegen**<br>In der Leistungsbeschreibung muss festgelegt werden, welche Nachweise (z. B. Zertifizierungen und Prüfberichte) unabhängiger Dritter zur Beurteilung des Cloud-Dienstes erforderlich sind.<br>Hierbei müssen die Ergebnisse der Datenkategorisierung und Risikoanalyse entsprechend berücksichtigt werden. | | |
| **2.1.2 Vertragliche Regelungen** | | **Hinweis:** Unterkapitel entfallen (Anforderungen nicht) |
| Vertragliche Regelungen nehmen bei der sicheren Nutzung von externen Cloud-Diensten eine zentrale Rolle ein. Daher benennen und konkretisieren die aufgeführten Mindestanforderungen zu regelnde Vertragsbestandteile aus Sicht der Informationssicherheit. Die Erfüllung der nachfolgenden Mindestanforderungen ist im Rahmen der Leistungsbeschreibung möglichst als Ausschlusskriterium zu fordern. | | I. Einleitungstext entfallen |
| **CD.07: Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern** | **NCD.2.2.02: Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern** | |
| Die Beteiligung von Unterauftragnehmern und anderen externen Dritten müssen vom Cloud-Anbieter vollständig in Art und Umfang benannt werden. | a) Die Einrichtung MUSS sich die Beteiligung von relevanten Unterauftragnehmern und anderen externen Dritten vom Cloud-Diensteanbieter vollständig in Art und | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise |
|---|---|---|
| Beabsichtigte Änderungen hierüber müssen unverzüglich schriftlich oder per E-Mail mitgeteilt werden.<br>Diese Mitteilungen können auch über Internetportale bereitgestellt werden, wenn dadurch die Anforderungen gleichwertig erfüllt sind (z. B. durch Push-Benachrichtigungen).<br>Falls Unterauftragnehmer nicht nur unwesentliche Teile zur Entwicklung oder zum Betrieb des Cloud-Dienstes beitragen, muss der Cloud-Anbieter zusichern,<br>– dass Unterauftragnehmer ebenfalls die vertraglich festgelegten Vorgaben erfüllen und<br>– dass zugesicherte Prüfrechte sich auch auf Unterauftragnehmer beziehen. | Umfang benennen lassen. Die Entscheidung, welcher Unterauftragnehmer hier zu nennen ist MUSS gemäß den Vorgaben des C5[xx] erfolgen.<br>[xx] Kriterienkatalog Cloud Computing (C5), (BSI 2020), Kap. 4.4.5, S.18f. | |
| | b) Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vereinbaren, dass beabsichtigte Änderungen hierüber unverzüglich schriftlich oder per E-Mail mitgeteilt werden. | |
| | c) Diese Mitteilungen KÖNNEN über Internetportale bereitgestellt werden, wenn dadurch die Anforderungen gleichwertig erfüllt sind (z. B. durch Push-Benachrichtigungen). | |
| | d) Falls Unterauftragnehmer wesentliche Teile[xx] zur Entwicklung oder zum Betrieb des Cloud-Dienstes beitragen, MUSS sich die Einrichtung vom Cloud-Diensteanbieter zusichern lassen, dass<br>– Unterauftragnehmer ebenfalls die vertraglich festgelegten Vorgaben erfüllen und<br>– zugesicherte Prüfrechte sich auch auf Unterauftragnehmer beziehen.<br>[xx] Hinsichtlich Bestimmung „wesentlicher Teile“ siehe C5, (BSI 2020a), S.91 | |
| **CD.08: Gerichtsbarkeit vertraglich zusichern** | **NCD.2.2.03: Gerichtsbarkeit vertraglich zusichern** | |
| Zur Absicherung der Verfügbarkeit als Teil der Informationssicherheit und soweit rechtlich möglich, müssen Vereinbarungen ausschließlich nach deutschem Recht und deutschem Gerichtsstand und ohne obligatorisch vorab zu betre bende Schlichtungsverfahren erfolgen. | a) Die Einrichtung SOLLTE zur Absicherung der Verfügbarkeit als Teil der Informationssicherheit Vereinbarungen ausschließlich nach deutschem Recht und deutschem Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren abschließen. | I. „SOLLTE“ anstatt „MÜSSEN“ |
| Es ist zu gewährleisten, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtsschutz keine Zeitverluste eintreten, zum Beispiel durch eine Einarbeitung in fremde Rechtsordnungen oder ein Auftreten vor entfernt gelegenen Gerichten,… | b) Die Einrichtung MUSS berücksichtigen, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtsschutz Zeitverluste eintreten können, insbesondere durch eine Einarbeitung in fremde Rechtsordnungen oder ein Auftreten vor entfernt gelegenen Gerichten. | |
| …so dass die Stelle des Bundes handlungsfähig bleibt und ihre Forderungen effektiv durchsetzen kann. | c) Die Einrichtung MUSS sicherstellen, dass sie handlungsfähig ble bt und ihre Forderungen effektiv durchsetzen kann. | |
| **CD.09: Lokation vertraglich zusichern** | **NCD.2.2.04: Lokation vertraglich zusichern** | |
| Sämtliche Lokationen, an denen Daten verarbeitet werden, sind vertraglich festzulegen. | a) Die Einrichtung MUSS sämtliche Lokationen, an denen dienstliche Daten verarbeitet werden, vertraglich festlegen. | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise |
|---|---|---|
| Ob die Daten an den vertraglich zugesicherten Lokationen verarbeitet werden dürfen, ist auf Basis der Ergebnisse der Datenkategorisierung und Risikoanalyse sowie der möglichen Gefahr eines fremdstaatlichen Zugriffs (z. B. durch Nachrichtendienste oder Ermittlungsbehörden) zu bewerten. | b) Die Einrichtung MUSS prüfen, ob die dienstlichen Daten an den vertraglich zugesicherten Lokationen verarbeitet werden dürfen. Dabei MUSS die Einrichtung die Ergebnisse der Datenkategorisierung und Ris koanalyse sowie der möglichen Gefahr eines fremdstaatlichen Zugriffs (z. B. durch Nachrichtendienste oder Ermittlungsbehörden) bewerten. | |
| **CD.10: Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern** | **NCD.2.2.0.5: Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern** | I. CD10 und CD11 zusammengelegt |
| Der Cloud-Anbieter muss zusichern, dass Daten nicht in den Bereich fremdstaatlicher Offenbarungspflichten und Ermittlungsbefugnisse gelangen.<br>Auf die geltenden Regelungen zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden wird in diesem Zusammenhang entsprechend verwiesen.xx<br>xx Vgl. BMI (2014), S.1 | a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter zusichern lassen, dass Daten nicht in den Bereich fremdstaatlicher Offenbarungspflichten und Ermittlungsbefugnisse gelangen.[xx]<br>[xx] Auf die geltenden Regelungen zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden wird in diesem Zusammenhang entsprechend verwiesen, (BMI 2014), S.1 | |
| **CD.11: weitere rechtliche Vereinbarungen vertraglich zusichern** | | |
| Pflichten des Cloud-Anbieters sicherheitsrelevante Vorfälle (sowie ggf. andere Vorfälle) gegenüber der Stelle des Bundes zu melden, müssen vertraglich geregelt sein. Vertragsstrafen und Haftungsfragen müssen in einem angemessenen Verhältnis zum ermittelten Schutzbedarf stehen. Bei der Festlegung sind die aus rechtlicher Sicht zulässigen Grenzen zu berücksichtigen. Vertragsstrafen sollten im Regelfall 5% des Auftragsvolumens nicht unterschreiten. | b) Die Einrichtung MUSS die Pflichten des Cloud-Diensteanbieters, sicherheitsrelevante Vorfälle (sowie ggf. andere Vorfälle) gegenüber der Einrichtung zu melden, vertraglich regeln.<br>i) Die Einrichtung MUSS bei Vertragsstrafen und Haftungsfragen auf ein angemessenes Verhältnis zum ermittelten Schutzbedarf achten.<br>ii) Bei der Festlegung sind die aus rechtlicher Sicht zulässigen Grenzen zu berücksichtigen. Die Einrichtung SOLLTE bei der Ansetzung von Vertragsstrafen 5% des Auftragsvolumens nicht unterschreiten. | |
| **CD.12: Beendigung des Vertragsverhältnisses regeln** | **NCD.2.2.06: Beendigung des Vertragsverhältnisses regeln** | |
| Kündigungsfristen müssen dem Einsatzszenario angemessen sein. | a) Die Einrichtung MUSS Kündigungsfristen dem Einsatzszenario angemessen festlegen. | |
| Soweit rechtlich möglich, müssen kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte an den Leistungen zu Lasten der Stelle des Bundes ausgeschlossen werden. | b) Soweit rechtlich möglich, MUSS die Einrichtung kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte an den Leistungen zu Lasten der Einrichtung ausschließen. | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise |
|---|---|---|
| **CD.13: Datenrückgabe und Datenlöschung beim Cloud-Anbieter vertraglich zusichern** | **NCD.2.2.07: Datenrückgabe und Datenlöschung beim Cloud-Diensteanbieter vertraglich zusichern** | |
| Die Rückgabe der Daten muss geregelt werden (Format, Datenträger, Protokolle, usw.). | a) Die Einrichtung MUSS die Rückgabe der Daten regeln (Format, Datenträger, Protokolle, usw.). | |
| Maßnahmen zur Datenlöschung müssen dem ermittelten Schutzbedarf entsprechen. | b) Die Einrichtung MUSS berücksichtigen, dass die Maßnahmen zur Datenlöschung dem ermittelten Schutzbedarf entsprechen. | |
| **2.2 Einsatzphase** | **2.3 Einsatzphase** | |
| Mindestanforderungen an den Cloud-Betrieb werden insbesondere durch die vertragliche Zusicherung der angemessenen und wirksamen Umsetzung des C5 (siehe Kapitel 2.1) aufgestellt. Sie adressieren primär den jeweiligen Cloud-Anbieter und gewährleisten damit einen sicheren Betrieb während der Vertragslaufzeit. Mindestanforderungen an den Einsatz von Cloud-Diensten regeln hingegen, wie die vertraglich zugesicherten Leistungen überwacht und überprüft werden können. Hierfür müssen Sicherheitsnachweise eingefordert und Informationspflichten des Cloud-Anbieters nachgehalten werden. Dies soll gewährleisten, dass die Stelle des Bundes die Risiken für ihre Informationssicherheit durch eigene Prüfungen, Auswertungen von Prüfberichten und sonstige vertraglich zur Verfügung gestellte Informationen des Cloud-Anbieters im Rahmen ihres Informationssicherheits-Management-Systems (ISMS) steuern kann. | Mindestanforderungen an den Einsatz von externen Cloud-Diensten regeln, wie die vertraglich zugesicherten Leistungen überwacht und überprüft werden. | **Hinweis:**<br>I. Text gekürzt |
| **CD.14: ISMS einbinden** | **NCD.2.3.01: ISMS einbinden** | |
| Die Stelle des Bundes muss den externen Cloud-Dienst in ihr eigenes ISMS einbinden. | a) Die Einrichtung MUSS den externen Cloud-Dienst in ihr eigenes Informationssicherheitsmanagementsystem (ISMS) einbinden. | |
| Sind durch die externe Cloud-Nutzung bei der Stelle des Bundes eigene Maßnahmen erforderlich, müssen diese umgesetzt werden. | b) Die Einrichtung MUSS die im C5-Bericht genannten korrespondierenden Kontrollen des Cloud-Dienstes bei sich einrichten. Die Einrichtung SOLLTE bei der Einbindung in das eigene ISMS zusätzlich die korrespondierenden Kriterien des C5[xx] berücksichtigen.<br><br>[xx] Hinweis: Der C5 führt mit Version 2020 Mitwirkungspflichten des Kunden als korrespondierende Kriterien ein. Die Umsetzung liegt im Verantwortungsbereich des Kunden und ist entscheidend für die Aufrechterhaltung der Informationssicherheit eines Cloud-Dienstes. Siehe C5, (BSI 2020a), S.9 | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise |
|---|---|---|
| **CD.15: Sicherheitsnachweise prüfen** | **NCD.2.3.02: Sicherheitsnachweise prüfen** | |
| Die Stelle des Bundes muss die Sicherheitsnachweise und sonstige Berichte des Cloud-Anbieters auswerten. Diese dürfen über den Nutzungszeitraum keine zeitlichen Lücken enthalten. Ergeben sich aus der Auswertung Unklarheiten, muss diesen nachgegangen werden. | a) Die Einrichtung MUSS die Nachweise und sonstige Berichte des Cloud-Diensteanbieters auswerten.[xx]<br>i) Diese DÜRFEN über den Nutzungszeitraum KEINE zeitlichen Lücken enthalten.<br>ii) Ergeben sich aus der Auswertung Unklarheiten, MUSS die Einrichtung diesen nachgehen.<br>[xx] Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“, (BSI 2020c), https://www.bsi.bund.de | I. Anpassung an Nachweise gem. Kapitel 2.1<br>II. Fußnote xx eingefügt. |
| Sofern erforderlich, sind die zugesicherten Prüf- und Kontrollrechte wahrzunehmen. | b) Die Einrichtung MUSS prüfen, ob festgestellte Unklarheiten durch Wahrnehmung der zugesicherten Prüf- und Kontrollrechte nachzugehen ist. | I. Jetzt Prüfung und Entscheidung durch Einrichtung! |
| **CD.16: Leistungsfähigkeit prüfen** | **NCD.2.3.03: Leistungsfähigkeit prüfen** | |
| Die Stelle des Bundes muss mindestens jährlich die Leistungsfähigkeiten ihrer eigenen IT-Infrastruktur, wie Performance der Netzanbindung und -verbindungen, überprüfen und ggf. anpassen. | a) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten ihrer eigenen IT-Infrastruktur, wie Performance der Netzanbindung und -verbindungen, beurteilen. | I. Jetzt „beurteilen“ anstatt „überprüfen“ |
| | b) Die Einrichtung MUSS auf Abweichungen reagieren und die eigene IT-Infrastruktur und Netzanbindung den Ergebnissen der Überprüfung anpassen. | I. Zusätzlich Reaktion auf Abweichungen. |
| | c) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten des Cloud-Diensteanbieter, wie Performance des Cloud-Services und die Netzverbindung zum Cloud-Diensteanbieter, beurteilen.[xx]<br>[xx] Hinweis: Viele Cloud-Diensteanbieter stellen diese Information kontinuierlich bereit, so dass diese Überprüfung als kontinuierliches Monitoring ausgestaltet werden kann. Mit dieser Anforderung ist gemeint, dass die vom Cloud-Diensteanbieter gelieferten oder von der Einrichtung erhobenen Daten zur Leistungsfähigkeit regelmäßig (mindestens jährlich) zu einer Beurteilung der Leistungsfähigkeit verdichtet und bewertet werden. | |
| **CD.17: Informationspflichten nachhalten** | **NCD.2.3.04: Informationspflichten nachhalten** | |
| Die Stelle des Bundes muss nachhalten, dass der Cloud-Anbieter seinen vertraglichen Informationspflichten stets nachkommt. Dies gilt insbesondere bei<br>– einer Eingliederung in ein anderes Unternehmen oder einen anderen Konzern oder in sonstigen Fällen des Wechsels des wirtschaftlichen Eigentums an ihn, | a) Die Einrichtung MUSS nachhalten, dass der Cloud-Diensteanbieter seinen vertraglichen Informationspflichten stets nachkommt. Dies gilt insbesondere bei<br>i) einer Eingliederung in ein anderes Unternehmen oder einen anderen Konzern oder in sonstigen Fällen des Wechsels des wirtschaftlichen Eigentums an ihn,<br>ii) einem Austausch von Unterauftragnehmern oder Dritten. | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise |
|---|---|---|
| – einem Austausch von Unterauftragnehmern oder Dritten. | | |
| | b) Die Einrichtung MUSS Meldungen des Cloud-Diensteanbieters über relevante Störungen und Cyber-Angriffe dokumentieren und gemäß den vereinbarten Mitwirkungspflichten nach NCD.2.2.01, Buchstabe c) reagieren.. | I. "Dokumentationspflicht in eigenen Buchstaben (Anforderung) |
| | **NCD.2.3.05: Zwei-Faktor-Authentifizierungen aktivieren** | **Hinweis:**<br>Neu hinzugefügt. |
| | a) Bietet der externe Cloud-Dienst eine Zwei-Faktor-Authentifizierung als Identitätsnachweis seiner Benutzer (Log-in) an, SOLLTE die Einrichtung diese nutzen. | **Hinweis:**<br>Als SOLLTE-Anforderung, da es 2FA-Lösungen geben könnte, die sich nicht in die IT der Einrichtung integrieren lassen könnte (z.B. SMS-Token) |
| **CD.18: Informationsaustausch** | | **Hinweis:**<br>entfallen. |
| Die Stelle des Bundes informiert das BSI über die eigene Nutzung externer Cloud-Dienste jährlich zum Stichtag 31. Januar. | | |
| Diese Informationen umfassen auch Beendigung und Wechsel von externen Cloud-Diensten.[xx]<br>[xx] für den standardisierten und vereinfachten Austausch siehe https:// www.bsi.bund.de | | |
| **2.3 Beendigungsphase** | **2.4 Beendigungsphase** | |
| Mindestanforderungen an die Beendigung der Cloud-Nutzung adressieren die ordnungsgemäße Abwicklung des Vertragsverhältnisses. Dies ist in der Regel nur möglich, wenn bereits bei Vertragsschluss alle relevanten Themen zum Vertragsende geregelt wurden. Daher umfasst bereits die Beschaffungsphase (Kapitel 2.1) entsprechende Mindestanforderungen zu diesem Bereich. | Mindestanforderungen an die Beendigung der Cloud-Nutzung adressieren die geordnete Beendigung des Vertragsverhältnisses.[xx]<br>[xx] siehe OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungsverhältnisses, (BSI 2020b), S.1ff | I: sprachliche Anpassung an IT-GS, hier OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses.<br>II. Text gekürzt |
| **CD.19: Datenrückgabe durchführen** | **NCD.2.4.01: Datenrückgabe durchführen** | |
| Alle Daten müssen vom Cloud-Anbieter in der vereinbarten Form zurück an die Stelle des Bundes übergeben werden. | a) Die Einrichtung MUSS prüfen, ob der Cloud-Diensteanbieter alle Daten in der vereinbarten Form zurück übergeben hat. | I. Prüfpflicht der Einrichtung |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise |
|---|---|---|
| Die Übergabe muss dokumentiert werden. | b) Die Einrichtung MUSS die Übergabe dokumentieren. | |
| **CD.20: Datenlöschung bestätigen** | **NCD.2.4.02: Datenlöschung bestätigen** | |
| Der Cloud-Anbieter muss die Löschung aller Daten der Stelle des Bundes, einschließlich vorhandener Datensicherungen, bestätigen. | a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter die Löschung aller Daten, einschließlich vorhandener Datensicherungen, bestätigen lassen. | I. Aktion jetzt bei der Einrichtung |
| Dies muss auch Daten und Datensicherungen bei möglichen Unterauftragnehmern und anderen externen Dritten umfassen. | b) Die Bestätigung nach Buchstabe a) MUSS auch Daten und Datensicherungen bei möglichen Unterauftragnehmern und anderen externen Dritten umfassen. | |
| Die Datenlöschung muss dokumentiert sein. | c) Die Einrichtung MUSS die Datenlöschung dokumentieren. | |
| | **2.5 Sicherheitsanforderungen bei einer Mitnutzung** | **Hinweis**: neues Kapitel; Mitnutzung war bisher in eigenen MST geregelt. |
| | Nehmen Benutzer einer Einrichtung einen externen Cloud-Dienst in Anspruch, ohne dass zwischen dieser Einrichtung und Cloud-Diensteanbieter ein Vertragsverhältnis besteht, geht dieser Mindeststandard von einer sog. Mitnutzung aus.[xx] Für diesen Anwendungsfall regeln die nachfolgenden Sicherheitsanforderungen das Mindestsicherheitsniveau.<br>[xx] Hinweis: Ein Akzeptieren von Allgemeinen Geschäftsbedingungen (AGB) oder sonstigen Nutzungsbedingungen sind nicht als ein Vertragsverhältnis im Sinne dieses Mindeststands anzusehen. | |
| | **NCD.2.5.01: Mitnutzung von externen Cloud-Diensten** | **Hinweis:** Anforderungen wurden aus Mindeststand zur **Mitnutzung** externer Cloud-Dienste übernommen und an die Modalverben angepasst. |
| Vormals Einleitungstext „Kapitel 2.1 Bewertung externer Cloud-Dienste“ | a) Die Einrichtung MUSS die Sicherheitsanforderungen nach NCD.2.1.03, Buchstaben d) bis i) umsetzen und einhalten. | **Hinweis:** Datenkategorisierung und Ris koanalyse |
| Vormals „MCD.2.1.03: Datenlokationen“<br>Es ist zu ermitteln, an welchen Lokationen Daten verarbeitet werden. Es ist zu bewerten, ob aus Sicht der mitnutzenden Behörde die Daten an den zugesicherten Lokationen verarbeitet werden dürfen. Hierfür sind insbesondere die Ergebnisse der Datenkategorisierung heranzuziehen. | b) Die Einrichtung MUSS ermitteln, an welchen Lokationen dienstliche Daten verarbeitet werden.<br>i) Die Einrichtung MUSS dann bewerten, ob aus ihrer Sicht die dienstlichen Daten an diesen Lokationen verarbeitet werden dürfen.<br>ii) Für diese Bewertung MUSS die Einrichtung insbesondere die Ergebnisse der Datenkategorisierung heranziehen. | |
| Vormals „MCD.2.1.04: Nutzung und Weitergabe von Daten an Dritte“ | c) Die Einrichtung MUSS ermitteln, welche Rechte dem Cloud-Diensteanbieter oder Dritten an den dienstlichen Daten eingeräumt werden. | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise |
|---|---|---|
| Es ist zu ermitteln, welche Rechte dem Cloud-Anbieter oder Dritten an den bzw. mit dem Umgang der Daten eingeräumt werden. Es ist zu bewerten, ob die Vereinbarungen und Bedingungen des Cloud-Anbieters mit den IT-Sicherheitsrichtlinien der mitnutzenden Behörde vereinbar sind. Hierzu sind insbesondere die Nutzungsbedingungen und die Datenschutzerklärung des Cloud-Anbieters auszuwerten. Rechte, aufgrund derer Daten an Dritte zu kommerziellen Zwecken verkauft oder selbst durch den Cloud-Anbieter außerhalb der konkreten, vorgesehenen Leistungserbringung genutzt werden können, sind im Regelfall nicht zu akzeptieren. | i) Die Einrichtung MUSS bewerten, ob diese Rechte mit der eigenen Sicherheitsrichtlinie vereinbar sind.<br>ii) Die Einrichtung MUSS insbesondere die Nutzungsbedingungen und die Datenschutzerklärung des Cloud-Diensteanbieters auswerten. | |
| Vormals „MCD.2.1.07: Verschlüsselung der Daten“<br>Es ist zu ermitteln, wie die Daten vom Cloud-Anbieter verschlüsselt gespeichert werden. Es ist zu bewerten, ob die Verschlüsselung mit den Anforderungen aus den Ergebnissen der Datenkategorisierung und Risikoanalyse vereinbar sind.17 Ist die vom Cloud-Anbieter eingesetzte Verschlüsselung nicht geeignet, ist zu prüfen, ob Anforderungen an die Vertraulichkeit der Daten über eine clientseitige Verschlüsselung erfüllt werden können. | d) Die Einrichtung MUSS ermitteln, wie die dienstlichen Daten im externen Cloud-Dienst verschlüsselt gespeichert werden.<br>i) Die Einrichtung MUSS dann bewerten, ob die Verschlüsselung mit den Anforderungen aus den Ergebnissen der Datenkategorisierung vereinbar sind.<br>ii) Ist die vom Cloud-Diensteanbieter eingesetzte Verschlüsselung nicht geeignet, MUSS die Einrichtung prüfen, ob Anforderungen an die Vertraulichkeit der Daten über eine clientseitige Verschlüsselung erfüllt werden können. | |
| Vormals „MCD.2.1.08: Erforderliche Softwareinstallationen“<br>Es ist zu ermitteln, ob für die Mitnutzung auf Arbeitsplatzcomputern oder mobilen Endgeräten der IT-Anwender zusätzliche Softwareinstallationen erforderlich sind. Es ist zu bewerten, ob die hierfür einzuräumenden Zugriffs- und Ausführungsrechte mit der Informationssicherheitsrichtlinie der mitnutzenden Behörde vereinbar sind und inwiefern gesonderte Lizenzen für die Mitnutzung eingeholt werden müssen.<br>Ist ein Zugriff über mobile Endgeräte geplant, sind diese zentral zu verwalten. Die Vorgaben des Mindeststandards Mobile Device Management sind zu beachten. | e) Die Einrichtung MUSS ermitteln, ob für die Mitnutzung auf den eigenen Arbeitsplatzcomputern oder mobilen Endgeräten zusätzliche Softwareinstallationen erforderlich sind.<br>i) Die Einrichtung MUSS dann bewerten, ob die hierfür einzuräumenden Zugriffs- und Ausführungsrechte mit der eigenen IT-Sicherheitsrichtlinie vereinbar sind und inwiefern gesonderte Lizenzen für die Mitnutzung eingeholt werden müssen.<br>ii) Ist ein Zugriff über mobile Endgeräte geplant, MUSS die Einrichtung diese zentral verwalten. Die Vorgaben des Mindeststandards Mobile Device Management sind zu beachten.[xx]<br>[xx] Siehe Mindeststandard des BSI Mobile Device Management, (BSI 2017) | |

**Von:** 1-IT-SI-0 [redacted]
**An:** GP Mindeststandards Bund
**Cc:** 1-IT-SI-L [redacted]; 1-IT-SI-R [redacted]
**Betreff:** AW: [MST NCD] Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2.0
**Datum:** Freitag, 8. Januar 2021 15:23:32
**Anlagen:** MST-NCD-RfC-Beta-Abgleich-V1.0.5_AA_01.docx

---

1-IT-SI-204.04/110

Sehr geehrte Damen und Herren,

anliegend erhalten Sie die mit Ihrem Schreiben BL35 - 750 00 07 vom 20.11.2020 erbetene Rückmeldung.

Neben den beigefügten, konkreten inhaltlichen Anmerkungen in der Spalte "Bemerkungen" bleibt grundsätzlich festzuhalten, dass der Mindeststandard zur (Mit-)Nutzung von Cloud-Diensten so zu formulieren ist, dass die praxisrelevanten Besonderheiten des Auswärtigen Amts, wie z. B. die Einhaltung des lokalen Rechts eines Gastlandes, Berücksichtigung finden.

Mit freundlichen Grüßen
[redacted]

IT-Sicherheitsmanagement

[redacted]@diplo.de

Auswärtiges Amt
Werderscher Markt 1
10117 Berlin

-----Ursprüngliche Nachricht-----
Von: [redacted]@bsi.bund.de] Im Auftrag von GP Geschaeftszimmer_BL
Gesendet: Freitag, 20. November 2020 11:06
An: poststelle@bk.bund.de - (Extern); Poststelle des AA; poststelle@bmi.bund.de; poststelle@bmf.bund.de - (Extern); poststelle@bmjv.bund.de; poststelle@bmvg.bund.de; info@bmwi.bund.de; poststelle@bmas.bund.de; poststelle@bmel.bund.de; poststelle@bmfsfj.bund.de - (Extern); poststelle@bmg.bund.de; poststelle@bmvi.bund.de; poststelle@bmu.bund.de; information@bmbf.bund.de; poststelle@bmz.bund.de; bverfg@bundesverfassungsgericht.de; poststelle@bpra.bund.de; bundesrat@bundesrat.de; Poststelle@brh.bund.de; [redacted]@bundestag.de; Poststelle@bkm.bund.de; poststelle@bfdi.bund.de - (Extern); [redacted]@itzbund.de; [redacted]@jm nrw.de; GP AG-InfoSic
Cc: GP Abteilung BL; GP Fachbereich BL 3; GP Referat BL 35; GP Poststelle; GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Geschaeftszimmer_BL
Betreff: [MST NCD] Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2.0

Sehr geehrte Damen und Herren,

anbei übersende ich Ihnen das Anschreiben sowie den Mindeststandard des BSI zur Nutzung externer Cloud-Dienste nach § 8 Absatz 1 Satz 1 BSIG - RfC-Beta-Version 1.0.5 vom 17.11.2020. Die Abgleichstabelle zum Mindeststandard ist der E-Mail ebenfalls beigefügt.

Mit freundlichen Grüßen
Im Auftrag

[redacted]

---
Geschäftszimmer BL
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 228 99 9582-[redacted]
Fax: +49 228 99 10 9582-[redacted]
E-Mail: geschaeftszimmer-bl@bsi.bund.de
Internet: www.bsi.bund.de
www.bsi-fuer-buerger.de

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| **1 Beschreibung** | **1 Beschreibung** | | |
| Dieser Mindeststandard definiert Sicherheitsanforderungen an die Nutzung externer Cloud-Dienste. | Dieser Mindeststandard setzt Sicherheitsanforderungen an die Nutzung externer Cloud-Dienste. | | |
| Diese Anforderungen sind einzuhalten, um ein Mindestmaß an Informationssicherheit beim Nutzen derartiger Dienste zu gewährleisten. | Die Erfüllung der im Mindeststandard vorgegebenen Sicherheitsanforderungen ist für ein angemessenes IT-Sicherheitsniveau notwendig, aber in der Regel nicht hinreichend.<br>Unter Berücksichtigung des individuellen Schutzbedarfs muss die Festlegung und Umsetzung eventuell zusätzlich erforderlicher Sicherheitsanforderungen erfolgen. | | |
| Er richtet sich hinsichtlich seiner Umsetzung an IT-Verantwortliche, IT-Sicherheitsbeauftragte[xx] und IT-Fachkräfte sowie mit der Beschaffung beauftragte Stellen.<br><br>[xx] Bzw. Informationssicherheitsbeauftragte | Er richtet sich hinsichtlich seiner Umsetzung an IT-Sicherheitsbeauftragte, IT-Betriebs- und Fachverantwortliche.[xx]<br><br>[xx] Rollen nach IT-Grundschutz-Kompendium, (BSI 2020b), S.1ff. | I. Wording IT-Grundschutz-Kompendium. Hier Rollen<br>II. Fußnote zu „Informationssicherheitsbeauftragter“ entfallen, jetzt im Vorwort<br>III. Fußnote Rollen nach IT-GS eingefügt. | Aus welchem Grund ist die Rolle Beschaffer entfallen? |
| Anbieter von Cloud-Diensten und andere interessierte Personen können diesen Mindeststandard zur Erhöhung der Informationssicherheit oder zum Abgleich ihrer Angebote heranziehen. | | I. Satz gestrichen, kein Regelungsinhalt. Gilt generell und wird auf der BSI-Webseite entsprechend klargestellt. | |
| | **1.1 Begriffsbestimmung und Abgrenzung** | I. Unterkapitel zur besseren Strukturierung eingeführt | |
| Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Insbesondere werden dabei Infrastrukturen, Plattformen und Software angeboten, die Spannbreite der angebotenen Cloud-Dienste umfasst darüber hinaus jedoch das komplette Spektrum der Informationstechnik.[xx]<br>[xx] BSI (2017), | Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Insbesondere werden dabei Infrastrukturen, Plattformen und Software angeboten, die Spannbreite der angebotenen Cloud-Dienste umfasst darüber hinaus jedoch das komplette Spektrum der Informationstechnik.[xx]<br>[xx] Definition nach https://www.bsi.bund.de/cloud | | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| https://www.bsi.bund.de/cloud External Link | | | |
| Externe Cloud-Dienste im Sinne dieses Mindeststandards sind im Rahmen von Cloud Computing angebotene Dienstleistungen, die über Netzwerke und Anbieter der Wirtschaft außerhalb der öffentlichen Verwaltung des Bundes und der Länder erbracht werden. | Externe Cloud-Dienste im Sinne dieses Mindeststandards sind im Rahmen von Cloud Computing angebotene Dienstleistungen, die über Netze und Anbieter der Wirtschaft außerhalb der öffentlichen Verwaltung des Bundes und der Länder erbracht werden.[XX]<br>[XY] Hinweis: IT-Dienstleistungen der „Bundescloud" fallen somit nicht unter diese Bestimmung. | I. Fußnote „Bundescloud" eingefügt | Die Begrifflichkeit „Bundescloud" muss allgemeiner gefasst werden, so dass auch weitere Clouds-Dienste des Bundes unter diese Vorgabe fallen.<br><br>Vorschlag: Die Formulierung sollte sich an der AG Cloud orientieren „Clouds des Bundes, der Länder und Kommunen". |
| Als Nutzung ist insbesondere die Beauftragung eines externen Cloud-Dienstes durch eine Stelle des Bundes selbst oder gemeinsam mit anderen zu verstehen. | Als Nutzung ist eine Verarbeitung von dienstlichen Daten[XX] durch einen externen Cloud-Dienst zu verstehen, der durch die Einrichtung selbst oder gemeinsam mit anderen beauftragt wird.<br><br>[XX] Dienstlich sind alle Daten, die im Rahmen der dienstlichen Tätigkeit erhoben und verarbeitet werden. Darunter fallen jedoch nicht personenbezogene Daten (wie Stammdaten, Nutzungsdaten), die für die Registrierung und Nutzung des Dienstes vom Cloud-Diensteanbieter erhoben oder verarbeitet werden. | I. Nutzungsbegriff auf „dienstliche Daten" konkretisiert<br>II. Fußnote „dienstliche Daten" hinzugefügt. | Der Begriff „dienstliche Daten" ist nicht hinreichend konkret definiert. Jedwede Daten, die bei der dienstlichen Nutzung externer Cloud-Dienste in einer Einrichtung verarbeitet werden, sind aus hiesiger Sicht als dienstliche Daten anzusehen.<br>Welche Daten außer personenbezogene Daten (wie Stammdaten, Nutzungsdaten) werden vom BSI bei der dienstlichen Nutzung von externen Cloud-Diensten als „nicht dienstlich" angesehen? |
| | Werden externe Cloud-Dienste durch Benutzer[xx] einer Einrichtung lediglich mitgenutzt, regelt Kapitel 2.5 den Umgang mit dienstlichen Daten in diesen Fällen entsprechend. Von einer Mitnutzung wird insbesondere ausgegangen, wenn die Einrichtung den externen Cloud-Diensten nicht beauftragt hat.<br>xx Analog Rolle „Benutzer" nach IT-Grundschutz-Kompendium, (BSI 2020b), S.31 | **Hinweis:**<br>Aufnahme zur Mitnutzung (siehe Kapitel 2.5) | Vorschlag: „[…], wenn eine Einrichtung die externen Cloud-Dienste nicht beauftragt hat." |
| | Werden keine dienstlichen Daten verarbeitet, können die Regelungen des Mindeststandards trotzdem angewendet werden (siehe NCD.2.1.03, Buchstabe e)). | I. Satz neu hinzugefügt. | Wenn keine dienstlichen Daten in einem externen Cloud-Dienst verarbeitet werden, welche anderen Arten von Daten (außer personenbezogener Daten) sieht das BSI bei einer dienstlichen Nutzung externer Cloud-Dienste? Bei der Nutzung externer Cloud-Dienste ohne einen dienstlichen Kontext entfällt der Regelungsbedarf. |
| | **1.2 Modalverben** | **Hinweis:** Einführung von Modalverben<br>Einheitlicher und abgestimmter Text. Bitte im Kapitel 1.2 keine Änderungen vornehmen! | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| Dieser Mindeststandard setzt die IT-Grundschutz-Vorgehensweise des BSI zum Management der Informationssicherheit voraus.[xx]<br>xx Vgl. BSI (2008), S.49f. | In Anlehnung an den IT-Grundschutz[xx] werden die Anforderungen mit den Modalverben „MUSS“ und „SOLLTE“ sowie den zugehörigen Verneinungen formuliert. Darüber hinaus wird das Modalverb KANN für ausgewählte Prüfaspekte verwendet.<br>[xx] Vgl. BSI-Standard 200-2, (BSI 2017), S.18 | | |
| Er gilt für alle Schutzbedarfskategorien. | Die hier genutzte Definition basiert auf RFC 2119[xx] und DIN 820-2: 2018[xy].<br>[xx] Vgl. Key words for use in RFCs to Indicate Requirement Levels, (IETF 1997)<br>[xy] Vgl. Normungsarbeit – Teil 2: Gestaltung von Dokumenten, (DIN 2018) | | |
| | **MUSS / DARF NUR**<br>bedeutet, dass diese Anforderung zwingend zu erfüllen ist. Das von der Nichtumsetzung ausgehende Risiko kann nicht im Rahmen einer Ris koanalyse akzeptiert werden. | | |
| | **DARF NICHT / DARF KEIN**<br>bedeutet, dass etwas zwingend zu unterlassen ist. Das durch die Umsetzung entstehende Risiko kann nicht im Rahmen einer Risikoanalyse akzeptiert werden. | | |
| | **SOLLTE**<br>bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können. | | Begründung der „Nicht-Umsetzung“ muss dokumentiert werden. |
| | **SOLLTE NICHT / SOLLTE KEIN**<br>bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können. | | Begründung der „Umsetzung“ muss dokumentiert werden. |
| | **KANN**<br>bedeutet, dass die Umsetzung / Nicht-Umsetzung optional ist und ohne Angabe von Gründen unterbleiben kann. | | |
| **2 Sicherheitsanforderungen** | **2 Sicherheitsanforderungen** | **Hinweis:** Die Reihenfolge der Sicherheitsanforderungen hat sich | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| | | gegenüber der V1.0 geändert.<br>Um diese dennoch leicht vergleichen zu können, sind die Anforderungen aus der V1.0 den Anforderungen aus V1.0.5 thematisch zugeordnet. | |
| Nachfolgende Sicherheitsanforderungen adressieren die Beschaffungs- (Kapitel 2.1), die Einsatz- (Kapitel 2.2) sowie die Beendigungsphase (Kapitel 2.3) von externen Cloud-Diensten. Diese sind einzuhalten, um ein Mindestmaß an Informationssicherheit zu gewährleisten. Sie können jedoch bei Bedarf durch zusätzliche Anforderungen erweitert werden. | Nachfolgende Sicherheitsanforderungen adressieren die Informationssicherheit entlang des gesamten Lebenszyklus und setzen auf den IT-Grundschutz-Baustein OPS.2.2 *Cloud-Nutzung*[xx] auf.<br>[xx] IT-Grundschutz-Kompendium, (BSI 2020b), OPS.2.2: *Cloud-Nutzung* | I. Einbindung des IT-Grundschutz-Bausteins OPS.2.2.<br>II. Text gekürzt. | |
| | **2.1. Planungsphase** | I. Planungsphase zur besseren Strukturierung eingeführt.<br>Hinweis: Bisher waren diese Regelungen als Erklärungstext implementiert. Diese sind jetzt als konkrete Anforderungen gesetzt! | |
| Vor der Nutzung externer Cloud-Dienste ist zusätzlich zur Schutzbedarfsfeststellung aus dem IT-Grundschutz eine vorgelagerte Datenkategorisierung und Risikoanalyse durchzuführen. | Grundlage der Informationssicherheit im Bereich Cloud Computing bilden nach dem IT-Grundschutz-Baustein OPS2.2 *Cloud-Nutzung*<br>– die Cloud-Nutzungs-Strategie<br>– die darauf basierende Sicherheitsrichtlinie sowie<br>– das jeweilige Sicherheitskonzept für den externen Cloud-Dienst.<br>Die nachfolgenden Sicherheitsanforderungen adressieren diese Dokumente entsprechend. | I. Bezug auf IT-GS, hier Cloud-Nutzungs-Strategie der Einrichtung, Sicherheitsrichtlinie und Sicherheitskonzept. | |
| | **NCD.2.1.01 Cloud-Nutzungs-Strategie** | **Hinweis:** OPS.2.2 fordert die Erstellung einer Cloud-Nutzungs-Strategie. Auf diese wird in der Sicherheitsanforderung verwiesen bzw. diese wird inhaltlich konkretisiert. | |
| | a) Die Einrichtung MUSS prüfen, ob der externe Cloud-Dienst grundsätzlich mit den in der Cloud-Nutzungs-Strategie definierten Zielen, Chancen und | | Vorschlag: „[…] grundsätzlich mit den in ihrer Cloud-Nutzungs-Strategie definierten Zielen, […]“ |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| | Ris ken vereinbar ist.[xx]<br>[xx] Hinweis: OPS.2.2.A1 Erstellung einer Cloud-Nutzungs-Strategie sieht die Erstellung einer Cloud-Nutzungs-Strategie vor. In dieser erfasst die Einrichtung ihre Ziele, Chancen und Risiken, die sie mit einer Cloud-Nutzung generell verbindet. Die Cloud-Nutzungs-Strategie nimmt daher eine zentrale Rolle für die Einrichtung ein. Sie wird benötigt, um die beabsichtigte Nutzung eines konkreten externen Cloud-Dienstes bewerten zu können. | | |
| | b) Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn Ziele, Chancen und Ris ken der Cloud-Nutzungs-Strategie angemessen berücksichtigt werden können. | | |
| | **NCD.2.1.02: Sicherheitsrichtlinie externe Cloud-Dienste** | **Hinweis**: OPS.2.2 fordert die Erstellung einer Sicherheitsrichtlinie. Auf diese wird in der Sicherheitsanforderung verwiesen bzw. diese wird inhaltlich konkretisiert. | |
| | a) Die Einrichtung MUSS eine Sicherheitsrichtlinie für externe Cloud-Dienste nach OPS.2.2.A2 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*[xx] erstellen.<br>[xx] IT-Grundschutz-Kompendium, (BSI 2020b), OPS.2.2: *Cloud-Nutzung* | **Hinweis:** War vorher in „CD.01: Systembeschre bung und weitergehende Informationen fordern“ enthalten!<br>(siehe weiter unten) | |
| | b) Die Einrichtung MUSS in dieser Sicherheitsrichtlinie mindestens die Umsetzung und Einhaltung der Basiskriterien nach dem Kriterienkatalog Cloud Computing (C5) als spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter festlegen.[xx]<br>[xx] Kriterienkatalog Cloud Computing (C5), (BSI 2020a), S.1ff. | I. hier werden jetzt die Basiskriterien des C5 verankert. Vorher war dies in der Leistungsbeschreibung. | Ein risikoorientiertes Vorgehen wird mit dieser Anforderung ausgeschlossen. Nicht für jedes Anwendungsszenario ist die Einhaltung der Basiskriterien des C5 Kriterienkatalogs notwendig oder auch möglich (z. B. ein durch eine Auslandsvertretung nach lokalem Recht des Gastlandes verpflichtend zu nutzender externer Cloud-Dienste Anbieter).<br>Da die C5 Kriterien aus etablierten Standards zur Informationssicherheit abgeleitet wurden, sollte es bei der Nutzung von Cloud-Diensten in einem Gastland möglich sein, die Umsetzung und Einhaltung von international anerkannten Standards/Kriterienkataloge (z. B. ISO 27001, SOC-2) als spezielle Sicherheitsanforderungen an einen Cloud- |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| | | | Diensteanbieter in der Sicherheitsrichtlinie festzulegen.<br><br>Es besteht weiterhin ein Widerspruch zur BSI IT-GS Anforderung „OPS.2.2.A13 Nachweis einer ausreichenden Informationssicherheit bei der Cloud-Nutzung“ hinsichtlich der verwendeten Modalverben:<br>▪ MST: „Die Einrichtung MUSS in dieser Sicherheitsrichtlinie [...]“<br>▪ OPS.2.2.A13: „Der Cloud-Kunde SOLLTE sich vom“<br><br>Auch handelt es sich im BSI IT-GS um eine Standardanforderung. Sind lediglich die Basis-Anforderungen umzusetzen, findet diese Anforderung im BSI IT-GS keine Anwendung, was im Widerspruch zum MST steht. |
| | c) Die Einrichtung MUSS die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragen bei der Erstellung der Sicherheitsrichtlinie beteiligen. | I. Beteiligung war vorher auf Risikoanalyse und Datenkategorisierung beschränkt! | |
| | **NCD.2.1.03: Sicherheitskonzept für den externen Cloud-Dienst** | | |
| | a) Die Einrichtung MUSS ein Sicherheitskonzept für den externen Cloud-Dienst nach OPS.2.2.A7 *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung* erstellen. | **Hinweis:** OPS.2.2 fordert die Erstellung eines Sicherheitskonzeptes. Auf dieses wird in der Sicherheitsanforderung verwiesen bzw. das Siko wird inhaltlich konkretisiert. | |
| Die Risikoanalyse ist insbesondere vor dem Hintergrund aktueller Veröffentlichungen des BSI zu Cloud-Sicherheit vorzunehmen.[xx]<br>[xx] Siehe hierzu insbesondere „Anforderungskatalog Cloud Computing des BSI“ (Cloud Computing Compliance Controls Catalogue, kurz C5). | b) Die Einrichtung MUSS in dem Sicherheitskonzept die aktuellen Veröffentlichungen des BSI zu Cloud-Sicherheit berücksichtigen.[xx]<br>[xx] siehe Veröffentlichungen unter https://www.bsi.bund.de/cloud | | |
| Im Rahmen dieser Risikoanalyse sind die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragen zu beteiligen. | c) Die Einrichtung MUSS die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragen bei der Erstellung des Sicherheitskonzeptes beteiligen. | I. jetzt Beteiligung bei Sicherheitskonzept, dies schließt dann Risikoanalyse und Datenkategorisierung mit ein! | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| | d) Die Einrichtung MUSS eine Datenkategorisierung durchführen, in der sämtliche dienstliche Daten identifiziert werden, die künftig in dem externen Cloud-Dienst verarbeitet werden sollen. | I. Feststellung, ob überhaupt dienstliche Daten verarbeitet werden sollen! | • Es wird auch an dieser Stelle die Abgrenzung zu „nicht-dienstlichen Daten" gefordert (s. o.).<br>• Die Durchführung der Datenkategorisierung wird auch unter g) beschrieben und gefordert, weshalb sie nicht bereits unter d) bei der Identifizierung der verarbeiteten Daten zu berücksichtigen wäre (Zirkelschluss).<br>o Vorschlag zur Änderung der Formulierung zu d): „Die Einrichtung MUSS sämtliche dienstliche Daten identifizieren, die künftig in dem externen Cloud-Dienst verarbeitet werden sollen.<br>• Um die Vorgabe praxistauglich und effizient zu gestalten, wird angeregt, eine Formulierung zu finden, welche die Identifikation der zukünftig zu verarbeitenden Informationen auf der Grundlage von Clustern (z. B. Nutzerdaten, Mitarbeiterdaten, Rechts- und Konsulardaten, Daten zur Abwicklung von Finanztransaktionen, etc.) vorsieht und nicht auf Einzeldatenebene, wie es aktuell der Fall ist. |
| | e) Kommt die Einrichtung zu dem Ergebnis, dass in dem externen Cloud-Dienst keine dienstlichen Daten verarbeitet werden, handelt es sich nicht um eine Nutzung oder Mitnutzung externer Cloud-Dienste im Sinne dieses Mindeststandards. In diesem Fällen KANN die Einrichtung die Sicherheitsanforderungen des Mindeststandards umsetzen. | I. Klarstellung, wann MST-Regelungen Anwendung finden! | |
| In der Datenkategorisierung sind zusätzlich zum Schutzbedarf Geheim- und Datenschutzaspekte[xx] sowie Personen- und Dienstgeheimnisse zu ermitteln.<br>[xx] Hinsichtlich Datenschutzaspekte siehe insbesondere AKTM (2011), S.1ff. | f) Die Einrichtung MUSS für die identifizierten dienstlichen Daten Geheim- und Datenschutzaspekte[xx] sowie Personen- und Dienstgeheimnisse ermitteln.<br>[xx] Hinsichtlich Datenschutzaspekte siehe insbesondere (AKTM 2011), S.1ff. | | Ist an dieser Stelle mit Personengeheimnis das unter g) beschriebene Privatgeheimnis gemeint? Wenn nicht, wieso werden unterschiedliche Begriffe verwendet? |
| Im Rahmen der Datenkategorisierung sind die Daten den nachfolgenden Kategorien zuzuordnen:<br>– Kategorie 1 = Privat- und Dienstgeheimnisse gemäß §§ 203 und 353b StGB<br>– Kategorie 2 = personenbezogene Daten gemäß § 3 Absatz 1 BDSG | g) Die Einrichtung MUSS die identifizierten dienstlichen Daten den nachfolgenden Kategorien zuordnen:<br>– Kategorie 1 = Privat- und Dienstgeheimnisse gemäß §§ 203 und 353b StGB<br>– Kategorie 2 = personenbezogene Daten gemäß § 3 Absatz 1 BDSG<br>– Kategorie 3 = Verschlusssachen gemäß | | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| – Kategorie 3 = Verschlusssachen gemäß allgemeiner Verwaltungsvorschrift des BMI zum materiellen und organisatorischen Schutz von Verschlusssachen (VSA)<br>– Kategorie 4 = sonstige Daten (weder Kategorie 1, noch 2, noch 3)<br>Daten können den Kategorien 1, 2 oder 3 gleichzeitig angehören. Die Kategorisierung der Daten ist zu dokumentieren. | Verschlusssachenanweisung - VSA[xx]<br>– Kategorie 4 = sonstige Daten (weder Kategorie 1, noch 2, noch 3)<br>h) Die Einrichtung KANN die identifizierten dienstlichen Daten den Kategorien 1, 2 oder 3 gleichzeitig zuordnen.<br>[xx] Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA), (BMI 2018) | | |
| | i) Die Einrichtung MUSS Risiken, die aus der künftigen Nutzung des externen Cloud-Dienstes entstehen können, umfassend ermitteln.[xx]<br>[xx] Hinweis: Bei dieser Prüfung geht es um eine anbieterunabhängige Prüfung. Es soll in diesem Zusammenhang geklärt werden, ob das beabsichtigte Cloud-Szenario mit der Cloud-Nutzung-Strategie vereinbar ist (z.B. Können die eigenen rechtlichen und organisatorischen Rahmenbedingungen überhaupt erfüllt werden?) | | |
| Die ermittelten Risiken für die Daten müssen betrachtet und bewertet werden. | i) Die Einrichtung MUSS die ermittelten Risiken mit denen in der eigenen Cloud-Nutzungs-Strategie (siehe NCD.2.1.01) festgelegten Richtlinien der Risikobewertung abgleichen und bewerten. | | |
| | ii) Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn die ermittelten Risiken gemäß der in der Cloud-Nutzungs-Strategie genannten Richtlinien zur Risikobewertung, wirksam vermieden oder hinreichend reduziert oder getragen werden können. | | |
| Auch auf Seiten der Stelle des Bundes können je nach Nutzungsszenario in allen Phasen der Cloud-Nutzung zusätzliche Maßnahmen erforderlich sein. | | **Hinweis:** keine Anforderung, sondern nur als Hinweistext. Wurde daher nicht übernommen | |
| | **NCD.2.1.04: Notfall- und Kontinuitätsmanagement** | **Hinweis:**<br>Anforderung neu hinzugefügt | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| | Mit Notfall- bzw. Kontinuitätsmanagement ist gemäß BSI-Standard 100-4[xx] ein Managementsystem zur Aufrechterhaltung einer definierten Arbeitsfähigkeit einer Einrichtung gemeint und umfasst sowohl präventive als auch reaktive Maßnahmen auf Notfälle und Krisensituationen. Es gilt im weiteren die Begrifflichkeit des BSI-Standards 100-4[xy].<br>[xx] BSI-Standard 100-4 – Notfallmanagement, (BSI 2008), S.1ff.<br>[xy] BSI-Standard 100-4 – Notfallmanagement, (BSI 2008), S.1ff. | **Hinweis:**<br>Nach Veröffentlichung von BSI 200-4 wird hier entsprechend angepasst. | |
| | a) Die Einrichtung MUSS prüfen, ob sie in Notfällen und Krisensituationen weiter auf den externen Cloud-Dienst zugreifen können muss.[xx]<br>[xx] Hinweis: Leitfragen für diese Prüfung können sein: Wird der Cloud-Dienst für einen, im Notfallmanagement als zeitkrisitsch bewerteten Geschäftsprozess (bzw. Fachaufgabe) genutzt? Dient der Cloud-Dienst zur Etablierung und Aufrechterhaltung eines Notbetriebs? Ist der Cloud-Dienst für die Bewältigung eines Notfalles relevant? | | Schreibfehler zeitkritisch |
| | b) Die Einrichtung MUSS bewerten, welche Bedeutung der externe Cloud-Dienst in Notfällen einnehmen würde.[xx]<br>xx Hinweis: Leitfragen für diese Prüfung können sein: Wie zeitkritisch sind die Geschäftsprozesse (bzw. Fachaufgaben), die den Cloud-Dienst in einem Notfall oder einer Krise benötigen? Zu welchem Grad wird der Cloud-Dienst in einem Notbetrieb benötigt? | | |
| | c) Die Einrichtung MUSS den zuständigen Notfallbeauftragten entsprechend einbinden. Dieser MUSS prüfen, ob die Prävention vor bzw. die Reaktion auf Notfälle oder Krisen durch die Cloud-Nutzung geändert werden muss. Die Einrichtung MUSS diese Änderungen vor der Cloud-Nutzung umsetzen. | | |
| **2.1 Beschaffungsphase** | **2.2 Beschaffungsphase** | | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| Ziel des Beschaffungsprozesses, für den die Vorgaben des Vergaberechts einschlägig sind, ist die Auswahl eines geeigneten Cloud-Anbieters. | Ziel des Beschaffungsprozesses, für den die Vorgaben des Vergaberechts einschlägig sind, ist die Auswahl eines geeigneten Cloud-Diensteanbieters. | I. Wording IT-GS (OPS.2.2 "Cloud-Nutzung"): Cloud-Anbieter durch Cloud-Diensteanbieter ersetzt. (Gilt für gesamte Dokument) | |
| **2.1.1 Auswahl Cloud-Anbieter** | | Unterkapitel entfallen | |
| Im Rahmen des Beschaffungsprozesses muss vom Bieter die Vorlage von Systembeschreibungen[xx], Zertifizierungen sowie Prüfberichten und anderen Nachweisen gefordert werden. Bei einer vorliegenden Testierung nach C5[xy] können die nachfolgend genannten Informationen aus der im Prüfbericht enthaltenen Systembeschreibung entnommen werden.<br>xx Beschreibung des Cloud-Dienste betreffenden internen Kontrollsystems (Systembeschreibung).<br>xy Vgl. BSI (2016), S.1ff. | | I. Einleitungstext entfallen, siehe Anforderung NCD.2.2.01, Buchstabe c) | |
| **CD.01: Systembeschreibung und weitergehende Informationen fordern** | **NCD.2.2.0.1: Umsetzung der Sicherheitsanforderungen** | **Hinweis:** Anforderungen zusammengefasst. | |
| | a) Die Einrichtung MUSS vor Vertragsabschluss überprüfen, ob die in ihrer Sicherheitsrichtlinie festgelegten Sicherheitsanforderungen (siehe NCD.2.1.02, Buchstabe a)) vom Cloud-Diensteanbieter erfüllt werden können.[xx]<br><br>[xx] Hinweis: Liegt ein Prüfbericht nach C5 vor, können diese Informationen daraus entnommen werden. | I. Konkretisierung auf die jeweilige Sicherheitsrichtlinie der Einrichtung<br>II. Hinweis auf Fundort in Fußnote. | |
| Die Vorlage der Systembeschre bung des Cloud-Dienstes muss in der Leistungsbeschreibung gefordert werden. | b) Die Einrichtung MUSS diese Sicherheitsanforderungen bereits in der Leistungsbeschreibung des externen Cloud-Dienstes einfordern. | | |
| Zur Beurteilung des Cloud-Anbieters können weitergehende Informationen im Rahmen der Leistungsbeschre bung gefordert werden. | | | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| Zudem sind mit Hilfe der Leistungsbeschreibung Basis- und Zusatzleistungen festzulegen. | | | |
| Sie muss die Vorgaben nach C5 erfüllen und ist insbesondere auf Mitwirkungspflichten und Maßnahmen hin zu prüfen. | | **Hinweis:** Die Festlegung auf die Kriterien des C5 erfolgt bereits in Anforderung NCD.2.2.01; Mitwirkungspflichten und Maßnahmen jetzt in Buchstabe c) | |
| **CD.03: Systembeschreibung und weitergehende Informationen auswerten**<br>Die Systembeschreibung und die weitergehenden Informationen müssen hinsichtlich Inhalt, Aussagekraft, Nachvollziehbarkeit, Aktualität und nachteiliger Regelungen ausgewertet werden.<br>Die Leistungsbeschre bung muss bereits genau definieren, welche Angaben vom Bieter erwartet werden.<br>Sofern die durch den Bieter vorgelegten Unterlagen Unklarheiten enthalten, muss geprüft werden, ob diese im Rahmen der Aufklärung aufzulösen sind oder zu Lasten des Bieters gehen. | c) Die Einrichtung MUSS die Angaben und Nachweise des Cloud-Diensteanbieters zu Buchstabe a) hinsichtlich Inhalt, Aussagekraft, Nachvollziehbarkeit, Aktualität, nachteiliger Regelungen sowie Mitwirkungspflichten und Maßnahmen auswerten. Dazu SOLLTE der „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“[xx] verwendet werden.<br>[xx] Hinweis: Der Auswertungsleitfaden gibt eine Struktur vor, welche die Einrichtung darin unterstützt, einen C5-Bericht systematisch auszuwerten. Dies beinhaltet, die Sicherheitsmaßnahmen des Cloud-Diensteanbieters (und die zugehörigen Prüfergebnisse) aufzunehmen, die eigenen Nutzerkontrollen für die Nutzung einzurichten und hierdurch das mit der Cloud-Nutzung verbundene Ris ko einzuschätzen und steuern zu können. Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“, (BSI 2020c), https://www.bsi.bund.de | **Hinweis:**<br>I. Anforderungstext gekürzt.<br><br>II. Auswerteleitfaden hinzugefügt | |
| **CD.04: Sicherheitsnachweise vertraglich zusichern**<br>Der Cloud-Anbieter muss regelmäßig Sicherheitsnachweise über<br>– die angemessene und wirksame Umsetzung der Basisanforderungen nach C5,<br>– die aktuelle Dokumentation der Systembeschre bung,<br>– die Aktualität von vertraglich zugesicherten Zertifizierungen sowie | d) Die Einrichtung MUSS sich die regelmäßige Vorlage von Sicherheitsnachweisen vom Cloud-Diensteanbieter zusichern lassen. | | |
| | e) Diese Sicherheitsnachweise SOLLTEN<br>– die angemessene und wirksame Umsetzung der Basiskriterien nach C5[xx],<br>– die aktuelle Dokumentation der Systembeschreibung,[xy]<br>– die Aktualität von vertraglich zugesicherten Zertifizierungen sowie<br>– die ordnungsgemäße Durchführung von | **Hinweis:**<br>I. Hinweis zur direkten Prüfung als Fußnote xy | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| – die ordnungsgemäße Durchführung von Datensicherungen und erprobten Rücksicherungen<br>vorlegen.<br>Diese Sicherheitsnachweise sollten durch die regelmäßige Bereitstellung des aktuellen Prüfberichtes nach C5 erbracht werden. Andere Nachweise bedürfen der begründeten Einzelfallentscheidung. | Datensicherungen und erprobten Rücksicherungen<br>umfassen und durch die regelmäßige Bereitstellung des aktuellen Prüfberichtes nach C5 erbracht werden. Andere Nachweise DARF die Einrichtung NUR in begründeten Einzelfallentscheidungen zulassen.<br>[xx] Hinweis: Die im C5 festgelegten Übergangsfristen für neue Versionen sind zu beachten.<br>[xy] Hinweis: Im Falle einer „direkten Prüfung" (vgl. C5, (BSI 2020), Kap. 4.4.5, S.16f.) enthält der Bericht keine Systembeschre bung vom Anbieter, sondern eine vom Prüfer im Rahmen der Prüfung erhobenen Beschreibung mit vergleichbarem Inhalt, die im Rahmen der Tätigkeiten dieses Mindeststandards herangezogen werden kann. | | |
| Prüfberichte und Nachweise dürfen über den Nutzungszeitraum keine zeitlichen Lücken enthalten. | f) Die Einrichtung MUSS die Sicherheitsnachweise des Cloud-Diensteanbieters auswerten. Insbesondere DÜRFEN Prüfberichte und Nachweise über den Nutzungszeitraum KEINE zeitlichen Lücken enthalten. | | |
| Die Einhaltung vorgesehener und vereinbarter Prozesse sowie die Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen durch den Cloud-Anbieter ist vertraglich zuzusichern. | g) Die Einrichtung MUSS sich die Einhaltung vorgesehener und vereinbarter Prozesse sowie die Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen durch den Cloud-Diensteanbieter vertraglich zusichern lassen. | | |
| **CD.05: Zusätzliche Anforderungen vertraglich zusichern**<br>Ermittelte Gefährdungen bzw. Risiken, die nicht bereits durch Basisanforderungen nach C5 abgedeckt sind, müssen über zusätzliche Anforderungen abgedeckt werden.<br>Für die zusätzlichen Anforderungen ist zu vereinbaren, dass regelmäßig geeignete Nachweise ihrer angemessenen und wirksamen Umsetzung vorgelegt werden.<br>Die Stelle des Bundes hat zu prüfen, ob sie weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) unterliegt, die | h) Die Einrichtung MUSS ermittelte Risiken, die nicht bereits durch die Basiskriterien nach C5 abgedeckt sind, über zusätzliche Anforderungen abdecken oder diese Risiken transferieren oder diese Risiken tragen.<br>i) Die Einrichtung MUSS prüfen, ob sie weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) unterliegt, die hinsichtlich der Cloud-Nutzung relevant sind. Diese Anforderungen MUSS die Einrichtung einhalten. Sie werden im Übrigen durch diesen Mindeststandard nicht berührt.<br>ii) Für die zusätzlichen Anforderungen MUSS die Einrichtung vereinbaren, dass regelmäßig | | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| hinsichtlich der Cloud-Nutzung relevant sind. Diese Anforderungen sind einzuhalten und werden im Übrigen durch diesen Mindeststandard nicht berührt. | geeignete Nachweise ihrer angemessenen und wirksamen Umsetzung vorgelegt werden. | | |
| **CD.06: Recht auf Prüfungen und Kontrollen vertraglich zusichern**<br>Grundsätzlich müssen der Stelle des Bundes eigene Prüfrechte vertraglich zugesichert werden.<br>Im Übrigen sind die Prüfrechte so auszugestalten, dass sie nach Art und Umfang einen Nachweis des Schutzniveaus ermöglichen und die Prüfung durch die Stelle des Bundes selbst oder durch Dritte in ihrem Auftrag (z. B. andere Stellen, externe IT-Revisoren oder Wirtschaftsprüfer) durchgeführt werden kann.<br>Aufgrund der Ergebnisse aus der Datenkategorisierung und Risikoanalyse kann in begründeten Ausnahmefällen auf eigene Prüfrechte verzichtet werden, soweit Rechtsvorschriften nicht entgegenstehen. Diese Entscheidung ist unter Ris kogesichtspunkten zu treffen und zu dokumentieren.<br>Sofern der Cloud-Anbieter keinen Prüfbericht nach C5 vorlegen kann, muss die Stelle des Bundes dazu berechtigt sein, die Prüfung nach C5 durch Dritte selbst beauftragen zu können. | I) Die Einrichtung SOLLTE sich eigene Prüfrechte vertraglich zusichern lassen.<br>i) Aufgrund der Ergebnisse aus der Datenkategorisierung und Risikoanalyse KANN die Einrichtung in begründeten Fällen auf eigene Prüfrechte verzichten, soweit Rechtsvorschriften nicht entgegenstehen.<br>ii) Die Einrichtung MUSS darauf achten, dass die Prüfrechte so ausgestaltet sind, dass die Einrichtung ihre gesetzlichen Anforderungen erfüllt.<br>iii) Die Einrichtung MUSS die Prüfrechte so ausgestalten, dass sie nach Art und Umfang einen Nachweis des Schutzniveaus ermöglichen und die Prüfung durch die Einrichtung selbst oder durch Dritte in ihrem Auftrag (z. B. andere Stellen, externe IT-Revisoren oder Wirtschaftsprüfer) durchgeführt werden kann.<br>iv) Sofern der Cloud-Diensteanbieter keinen Prüfbericht nach C5 vorlegen kann, MUSS die Einrichtung dazu berechtigt sein, die Prüfung nach C5 durch Dritte selbst beauftragen zu können. | | |
| **CD.02: Zertifizierungen oder Bescheinigungen unabhängiger Dritter festlegen**<br>In der Leistungsbeschreibung muss festgelegt werden, welche Nachweise (z. B. Zertifizierungen und Prüfberichte) unabhängiger Dritter zur Beurteilung des Cloud-Dienstes erforderlich sind.<br>Hierbei müssen die Ergebnisse der Datenkategorisierung und Risikoanalyse entsprechend berücksichtigt werden. | | | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| **2.1.2 Vertragliche Regelungen** | | **Hinweis:** Unterkapitel entfallen (Anforderungen nicht) | |
| Vertragliche Regelungen nehmen bei der sicheren Nutzung von externen Cloud-Diensten eine zentrale Rolle ein. Daher benennen und konkretisieren die aufgeführten Mindestanforderungen zu regelnde Vertragsbestandteile aus Sicht der Informationssicherheit. Die Erfüllung der nachfolgenden Mindestanforderungen ist im Rahmen der Leistungsbeschreibung möglichst als Ausschlusskriterium zu fordern. | | I. Einleitungstext entfallen | |
| **CD.07: Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern** | **NCD.2.2.02: Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern** | | |
| Die Beteiligung von Unterauftragnehmern und anderen externen Dritten müssen vom Cloud-Anbieter vollständig in Art und Umfang benannt werden.<br>Beabsichtigte Änderungen hierüber müssen unverzüglich schriftlich oder per E-Mail mitgeteilt werden.<br>Diese Mitteilungen können auch über Internetportale bereitgestellt werden, wenn dadurch die Anforderungen gleichwertig erfüllt sind (z. B. durch Push-Benachrichtigungen).<br>Falls Unterauftragnehmer nicht nur unwesentliche Teile zur Entwicklung oder zum Betrieb des Cloud-Dienstes beitragen, muss der Cloud-Anbieter zusichern,<br>– dass Unterauftragnehmer ebenfalls die vertraglich festgelegten Vorgaben erfüllen und<br>– dass zugesicherte Prüfrechte sich auch auf Unterauftragnehmer beziehen. | a) Die Einrichtung MUSS sich die Beteiligung von relevanten Unterauftragnehmern und anderen externen Dritten vom Cloud-Diensteanbieter vollständig in Art und Umfang benennen lassen. Die Entscheidung, welcher Unterauftragnehmer hier zu nennen ist MUSS gemäß den Vorgaben des C5[xx] erfolgen.<br>[xx] Kriterienkatalog Cloud Computing (C5), (BSI 2020), Kap. 4.4.5, S.18f. | | |
| | b) Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vereinbaren, dass beabsichtigte Änderungen hierüber unverzüglich schriftlich oder per E-Mail mitgeteilt werden. | | |
| | c) Diese Mitteilungen KÖNNEN über Internetportale bereitgestellt werden, wenn dadurch die Anforderungen gleichwertig erfüllt sind (z. B. durch Push-Benachrichtigungen). | | |
| | d) Falls Unterauftragnehmer wesentliche Teile[xx] zur Entwicklung oder zum Betrieb des Cloud-Dienstes beitragen, MUSS sich die Einrichtung vom Cloud-Diensteanbieter zusichern lassen, dass<br>– Unterauftragnehmer ebenfalls die vertraglich festgelegten Vorgaben erfüllen | | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| | und<br>– zugesicherte Prüfrechte sich auch auf Unterauftragnehmer beziehen.<br>[xx] Hinsichtlich Bestimmung „wesentlicher Teile" siehe C5, (BSI 2020a), S.91 | | |
| **CD.08: Gerichtsbarkeit vertraglich zusichern** | **NCD.2.2.03: Gerichtsbarkeit vertraglich zusichern** | | |
| Zur Absicherung der Verfügbarkeit als Teil der Informationssicherheit und soweit rechtlich möglich, müssen Vereinbarungen ausschließlich nach deutschem Recht und deutschem Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren erfolgen. | a) Die Einrichtung SOLLTE zur Absicherung der Verfügbarkeit als Teil der Informationssicherheit Vereinbarungen ausschließlich nach deutschem Recht und deutschem Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren abschließen. | I. „SOLLTE" anstatt „MÜSSEN" | |
| Es ist zu gewährleisten, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtsschutz keine Zeitverluste eintreten, zum Beispiel durch eine Einarbeitung in fremde Rechtsordnungen oder ein Auftreten vor entfernt gelegenen Gerichten,… | b) Die Einrichtung MUSS berücksichtigen, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtsschutz Zeitverluste eintreten können, insbesondere durch eine Einarbeitung in fremde Rechtsordnungen oder ein Auftreten vor entfernt gelegenen Gerichten. | | |
| …so dass die Stelle des Bundes handlungsfähig bleibt und ihre Forderungen effektiv durchsetzen kann. | c) Die Einrichtung MUSS sicherstellen, dass sie handlungsfähig bleibt und ihre Forderungen effektiv durchsetzen kann. | | |
| **CD.09: Lokation vertraglich zusichern** | **NCD.2.2.04: Lokation vertraglich zusichern** | | |
| Sämtliche Lokationen, an denen Daten verarbeitet werden, sind vertraglich festzulegen. | a) Die Einrichtung MUSS sämtliche Lokationen, an denen dienstliche Daten verarbeitet werden, vertraglich festlegen. | | |
| Ob die Daten an den vertraglich zugesicherten Lokationen verarbeitet werden dürfen, ist auf Basis der Ergebnisse der Datenkategorisierung und Risikoanalyse sowie der möglichen Gefahr eines fremdstaatlichen Zugriffs (z. B. durch Nachrichtendienste oder Ermittlungsbehörden) zu bewerten. | b) Die Einrichtung MUSS prüfen, ob die dienstlichen Daten an den vertraglich zugesicherten Lokationen verarbeitet werden dürfen. Dabei MUSS die Einrichtung die Ergebnisse der Datenkategorisierung und Risikoanalyse sowie der möglichen Gefahr eines fremdstaatlichen Zugriffs (z. B. durch Nachrichtendienste oder Ermittlungsbehörden) bewerten. | | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| **CD.10: Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern** | **NCD.2.2.0.5: Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern** | I. CD10 und CD11 zusammengelegt | |
| Der Cloud-Anbieter muss zusichern, dass Daten nicht in den Bereich fremdstaatlicher Offenbarungspflichten und Ermittlungsbefugnisse gelangen.<br>Auf die geltenden Regelungen zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden wird in diesem Zusammenhang entsprechend verwiesen.xx<br>xx Vgl. BMI (2014), S.1 | a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter zusichern lassen, dass Daten nicht in den Bereich fremdstaatlicher Offenbarungspflichten und Ermittlungsbefugnisse gelangen.[xx]<br><br>[xx] Auf die geltenden Regelungen zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden wird in diesem Zusammenhang entsprechend verwiesen, (BMI 2014), S.1 | | Die Formulierung unterbindet ein ris koorientiertes, abgestuftes Vorgehen in Abhängigkeit zum tatsächlichen Schutzbedarf der bei einem Cloud-Dienst verarbeiteten „dienstlichen" Daten.<br><br>Bsp.: Die Nutzung eines Cloud-Dienstes zur Sammlung/zum Zusammentragen öffentlich verfügbarer Informationen hat einen geringeren Schutzbedarf als die Verarbeitung vertraulicher dienstlicher Informationen. |
| **CD.11: weitere rechtliche Vereinbarungen vertraglich zusichern** | | | |
| Pflichten des Cloud-Anbieters sicherheitsrelevante Vorfälle (sowie ggf. andere Vorfälle) gegenüber der Stelle des Bundes zu melden, müssen vertraglich geregelt sein. Vertragsstrafen und Haftungsfragen müssen in einem angemessenen Verhältnis zum ermittelten Schutzbedarf stehen. Bei der Festlegung sind die aus rechtlicher Sicht zulässigen Grenzen zu berücksichtigen. Vertragsstrafen sollten im Regelfall 5% des Auftragsvolumens nicht unterschreiten. | b) Die Einrichtung MUSS die Pflichten des Cloud-Diensteanbieters, sicherheitsrelevante Vorfälle (sowie ggf. andere Vorfälle) gegenüber der Einrichtung zu melden, vertraglich regeln.<br>i) Die Einrichtung MUSS bei Vertragsstrafen und Haftungsfragen auf ein angemessenes Verhältnis zum ermittelten Schutzbedarf achten.<br>ii) Bei der Festlegung sind die aus rechtlicher Sicht zulässigen Grenzen zu berücksichtigen. Die Einrichtung SOLLTE bei der Ansetzung von Vertragsstrafen 5% des Auftragsvolumens nicht unterschreiten. | | |
| **CD.12: Beendigung des Vertragsverhältnisses regeln** | **NCD.2.2.06: Beendigung des Vertragsverhältnisses regeln** | | |
| Kündigungsfristen müssen dem Einsatzszenario angemessen sein. | a) Die Einrichtung MUSS Kündigungsfristen dem Einsatzszenario angemessen festlegen. | | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| Soweit rechtlich möglich, müssen kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte an den Leistungen zu Lasten der Stelle des Bundes ausgeschlossen werden. | b) Soweit rechtlich möglich, MUSS die Einrichtung kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte an den Leistungen zu Lasten der Einrichtung ausschließen. | | |
| **CD.13: Datenrückgabe und Datenlöschung beim Cloud-Anbieter vertraglich zusichern** | **NCD.2.2.07: Datenrückgabe und Datenlöschung beim Cloud-Diensteanbieter vertraglich zusichern** | | |
| Die Rückgabe der Daten muss geregelt werden (Format, Datenträger, Protokolle, usw.). | a) Die Einrichtung MUSS die Rückgabe der Daten regeln (Format, Datenträger, Protokolle, usw.). | | |
| Maßnahmen zur Datenlöschung müssen dem ermittelten Schutzbedarf entsprechen. | b) Die Einrichtung MUSS berücksichtigen, dass die Maßnahmen zur Datenlöschung dem ermittelten Schutzbedarf entsprechen. | | |
| **2.2 Einsatzphase** | **2.3 Einsatzphase** | | |
| Mindestanforderungen an den Cloud-Betrieb werden insbesondere durch die vertragliche Zusicherung der angemessenen und wirksamen Umsetzung des C5 (siehe Kapitel 2.1) aufgestellt. Sie adressieren primär den jeweiligen Cloud-Anbieter und gewährleisten damit einen sicheren Betrieb während der Vertragslaufzeit. Mindestanforderungen an den Einsatz von Cloud-Diensten regeln hingegen, wie die vertraglich zugesicherten Leistungen überwacht und überprüft werden können. Hierfür müssen Sicherheitsnachweise eingefordert und Informationspflichten des Cloud-Anbieters nachgehalten werden. Dies soll gewährleisten, dass die Stelle des Bundes die Risiken für ihre Informationssicherheit durch eigene Prüfungen, Auswertungen von Prüfberichten und sonstige vertraglich zur Verfügung gestellte Informationen des Cloud-Anbieters im Rahmen ihres Informationssicherheits-Management-Systems (ISMS) steuern kann. | Mindestanforderungen an den Einsatz von externen Cloud-Diensten regeln, wie die vertraglich zugesicherten Leistungen überwacht und überprüft werden. | **Hinweis:**<br>I. Text gekürzt | |
| **CD.14: ISMS einbinden** | **NCD.2.3.01: ISMS einbinden** | | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| Die Stelle des Bundes muss den externen Cloud-Dienst in ihr eigenes ISMS einbinden. | a) Die Einrichtung MUSS den externen Cloud-Dienst in ihr eigenes Informationssicherheitsmanagementsystem (ISMS) einbinden. | | Die Formulierung unterbindet ein ris koorientiertes, abgestuftes Vorgehen in Abhängigkeit zum tatsächlichen Schutzbedarf der bei einem Cloud-Dienst verarbeiteten „dienstlichen" Daten.<br><br>Bsp.: Die Nutzung eines Cloud-Dienstes zur Sammlung/zum Zusammentragen öffentlich verfügbarer Informationen hat einen geringeren Schutzbedarf als die Verarbeitung vertraulicher dienstlicher Informationen. |
| Sind durch die externe Cloud-Nutzung bei der Stelle des Bundes eigene Maßnahmen erforderlich, müssen diese umgesetzt werden. | b) Die Einrichtung MUSS die im C5-Bericht genannten korrespondierenden Kontrollen des Cloud-Dienstes bei sich einrichten. Die Einrichtung SOLLTE bei der Einbindung in das eigene ISMS zusätzlich die korrespondierenden Kriterien des C5[xx] berücksichtigen.<br><br>[xx] Hinweis: Der C5 führt mit Version 2020 Mitwirkungspflichten des Kunden als korrespondierende Kriterien ein. Die Umsetzung liegt im Verantwortungsbereich des Kunden und ist entscheidend für die Aufrechterhaltung der Informationssicherheit eines Cloud-Dienstes. Siehe C5, (BSI 2020a), S.9 | | |
| **CD.15: Sicherheitsnachweise prüfen** | **NCD.2.3.02: Sicherheitsnachweise prüfen** | | |
| Die Stelle des Bundes muss die Sicherheitsnachweise und sonstige Berichte des Cloud-Anbieters auswerten. Diese dürfen über den Nutzungszeitraum keine zeitlichen Lücken enthalten. Ergeben sich aus der Auswertung Unklarheiten, muss diesen nachgegangen werden. | a) Die Einrichtung MUSS die Nachweise und sonstige Berichte des Cloud-Diensteanbieters auswerten.[xx]<br>i) Diese DÜRFEN über den Nutzungszeitraum KEINE zeitlichen Lücken enthalten.<br>ii) Ergeben sich aus der Auswertung Unklarheiten, MUSS die Einrichtung diesen nachgehen.<br>[xx] Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5", (BSI 2020c), https://www.bsi.bund.de | I. Anpassung an Nachweise gem. Kapitel 2.1<br>II. Fußnote xx eingefügt. | |
| Sofern erforderlich, sind die zugesicherten Prüf- und Kontrollrechte wahrzunehmen. | b) Die Einrichtung MUSS prüfen, ob festgestellte Unklarheiten durch Wahrnehmung der zugesicherten Prüf- und Kontrollrechte nachzugehen ist. | I. Jetzt Prüfung und Entscheidung durch Einrichtung! | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| **CD.16: Leistungsfähigkeit prüfen** | **NCD.2.3.03: Leistungsfähigkeit prüfen** | | |
| Die Stelle des Bundes muss mindestens jährlich die Leistungsfähigkeiten ihrer eigenen IT-Infrastruktur, wie Performance der Netzanbindung und -verbindungen, überprüfen und ggf. anpassen. | a) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten ihrer eigenen IT-Infrastruktur, wie Performance der Netzanbindung und -verbindungen, beurteilen. | I. Jetzt „beurteilen“ anstatt „überprüfen“ | |
| | b) Die Einrichtung MUSS auf Abweichungen reagieren und die eigene IT-Infrastruktur und Netzanbindung den Ergebnissen der Überprüfung anpassen. | I. Zusätzlich Reaktion auf Abweichungen. | |
| | c) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten des Cloud-Diensteanbieter, wie Performance des Cloud-Services und die Netzverbindung zum Cloud-Diensteanbieter, beurteilen.[xx]<br>[xx] Hinweis: Viele Cloud-Diensteanbieter stellen diese Information kontinuierlich bereit, so dass diese Überprüfung als kontinuierliches Monitoring ausgestaltet werden kann. Mit dieser Anforderung ist gemeint, dass die vom Cloud-Diensteanbieter gelieferten oder von der Einrichtung erhobenen Daten zur Leistungsfähigkeit regelmäßig (mindestens jährlich) zu einer Beurteilung der Leistungsfähigkeit verdichtet und bewertet werden. | | |
| **CD.17: Informationspflichten nachhalten** | **NCD.2.3.04: Informationspflichten nachhalten** | | |
| Die Stelle des Bundes muss nachhalten, dass der Cloud-Anbieter seinen vertraglichen Informationspflichten stets nachkommt. Dies gilt insbesondere bei<br>– einer Eingliederung in ein anderes Unternehmen oder einen anderen Konzern oder in sonstigen Fällen des Wechsels des wirtschaftlichen Eigentums an ihn,<br>– einem Austausch von Unterauftragnehmern oder Dritten. | a) Die Einrichtung MUSS nachhalten, dass der Cloud-Diensteanbieter seinen vertraglichen Informationspflichten stets nachkommt. Dies gilt insbesondere bei<br>i) einer Eingliederung in ein anderes Unternehmen oder einen anderen Konzern oder in sonstigen Fällen des Wechsels des wirtschaftlichen Eigentums an ihn,<br>ii) einem Austausch von Unterauftragnehmern oder Dritten. | | |
| | b) Die Einrichtung MUSS Meldungen des Cloud-Diensteanbieters über relevante Störungen und Cyber-Angriffe dokumentieren und gemäß den | I. "Dokumentationspflicht in eigenen Buchstaben (Anforderung) | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| | vereinbarten Mitwirkungspflichten nach NCD.2.2.01, Buchstabe c) reagieren.. | | |
| | **NCD.2.3.05: Zwei-Faktor-Authentifizierungen aktivieren** | **Hinweis:**<br>Neu hinzugefügt. | |
| | a) Bietet der externe Cloud-Dienst eine Zwei-Faktor-Authentifizierung als Identitätsnachweis seiner Benutzer (Log-in) an, SOLLTE die Einrichtung diese nutzen. | **Hinweis:**<br>Als SOLLTE-Anforderung, da es 2FA-Lösungen geben könnte, die sich nicht in die IT der Einrichtung integrieren lassen könnte (z.B. SMS-Token) | |
| **CD.18: Informationsaustausch** | | **Hinweis:**<br>entfallen. | |
| Die Stelle des Bundes informiert das BSI über die eigene Nutzung externer Cloud-Dienste jährlich zum Stichtag 31. Januar. | | | |
| Diese Informationen umfassen auch Beendigung und Wechsel von externen Cloud-Diensten.[xx]<br>[xx] für den standardisierten und vereinfachten Austausch siehe https://www.bsi.bund.de | | | |
| **2.3 Beendigungsphase** | **2.4 Beendigungsphase** | | |
| Mindestanforderungen an die Beendigung der Cloud-Nutzung adressieren die ordnungsgemäße Abwicklung des Vertragsverhältnisses. Dies ist in der Regel nur möglich, wenn bereits bei Vertragsschluss alle relevanten Themen zum Vertragsende geregelt wurden. Daher umfasst bereits die Beschaffungsphase (Kapitel 2.1) entsprechende Mindestanforderungen zu diesem Bereich. | Mindestanforderungen an die Beendigung der Cloud-Nutzung adressieren die geordnete Beendigung des Vertragsverhältnisses.[xx]<br>[xx] siehe OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungsverhältnisses, (BSI 2020b), S.1ff | I: sprachliche Anpassung an IT-GS, hier OPS.2.2.A14 Geordnete Beendigung eines Cloud-Nutzungs-Verhältnisses.<br>II. Text gekürzt | |
| **CD.19: Datenrückgabe durchführen** | **NCD.2.4.01: Datenrückgabe durchführen** | | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| Alle Daten müssen vom Cloud-Anbieter in der vereinbarten Form zurück an die Stelle des Bundes übergeben werden. | a) Die Einrichtung MUSS prüfen, ob der Cloud-Diensteanbieter alle Daten in der vereinbarten Form zurück übergeben hat. | I. Prüfpflicht der Einrichtung | |
| Die Übergabe muss dokumentiert werden. | b) Die Einrichtung MUSS die Übergabe dokumentieren. | | |
| **CD.20: Datenlöschung bestätigen** | **NCD.2.4.02: Datenlöschung bestätigen** | | |
| Der Cloud-Anbieter muss die Löschung aller Daten der Stelle des Bundes, einschließlich vorhandener Datensicherungen, bestätigen. | a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter die Löschung aller Daten, einschließlich vorhandener Datensicherungen, bestätigen lassen. | I. Aktion jetzt bei der Einrichtung | |
| Dies muss auch Daten und Datensicherungen bei möglichen Unterauftragnehmern und anderen externen Dritten umfassen. | b) Die Bestätigung nach Buchstabe a) MUSS auch Daten und Datensicherungen bei möglichen Unterauftragnehmern und anderen externen Dritten umfassen. | | |
| Die Datenlöschung muss dokumentiert sein. | c) Die Einrichtung MUSS die Datenlöschung dokumentieren. | | |
| | **2.5 Sicherheitsanforderungen bei einer Mitnutzung** | **Hinweis**: neues Kapitel; Mitnutzung war bisher in eigenen MST geregelt. | |
| | Nehmen Benutzer einer Einrichtung einen externen Cloud-Dienst in Anspruch, ohne dass zwischen dieser Einrichtung und Cloud-Diensteanbieter ein Vertragsverhältnis besteht, geht dieser Mindeststandard von einer sog. Mitnutzung aus.[xx] Für diesen Anwendungsfall regeln die nachfolgenden Sicherheitsanforderungen das Mindestsicherheitsniveau.<br>[xx] Hinweis: Ein Akzeptieren von Allgemeinen Geschäftsbedingungen (AGB) oder sonstigen Nutzungsbedingungen sind nicht als ein Vertragsverhältnis im Sinne dieses Mindeststands anzusehen. | | |
| | **NCD.2.5.01: Mitnutzung von externen Cloud-Diensten** | **Hinweis:** Anforderungen wurden aus Mindeststand zur **Mitnutzung** externer Cloud-Dienste übernommen und an die Modalverben angepasst. | |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| Vormals Einleitungstext „Kapitel 2.1 Bewertung externer Cloud-Dienste“ | a) Die Einrichtung MUSS die Sicherheitsanforderungen nach NCD.2.1.03, Buchstaben d) bis i) umsetzen und einhalten. | **Hinweis:** Datenkategorisierung und Risikoanalyse | |
| Vormals „MCD.2.1.03: Datenlokationen“<br>Es ist zu ermitteln, an welchen Lokationen Daten verarbeitet werden. Es ist zu bewerten, ob aus Sicht der mitnutzenden Behörde die Daten an den zugesicherten Lokationen verarbeitet werden dürfen. Hierfür sind insbesondere die Ergebnisse der Datenkategorisierung heranzuziehen. | b) Die Einrichtung MUSS ermitteln, an welchen Lokationen dienstliche Daten verarbeitet werden.<br>i) Die Einrichtung MUSS dann bewerten, ob aus ihrer Sicht die dienstlichen Daten an diesen Lokationen verarbeitet werden dürfen.<br>ii) Für diese Bewertung MUSS die Einrichtung insbesondere die Ergebnisse der Datenkategorisierung heranziehen. | | |
| Vormals „MCD.2.1.04: Nutzung und Weitergabe von Daten an Dritte“<br>Es ist zu ermitteln, welche Rechte dem Cloud-Anbieter oder Dritten an den bzw. mit dem Umgang der Daten eingeräumt werden. Es ist zu bewerten, ob die Vereinbarungen und Bedingungen des Cloud-Anbieters mit den IT-Sicherheitsrichtlinien der mitnutzenden Behörde vereinbar sind. Hierzu sind insbesondere die Nutzungsbedingungen und die Datenschutzerklärung des Cloud-Anbieters auszuwerten. Rechte, aufgrund derer Daten an Dritte zu kommerziellen Zwecken verkauft oder selbst durch den Cloud-Anbieter außerhalb der konkreten, vorgesehenen Leistungserbringung genutzt werden können, sind im Regelfall nicht zu akzeptieren. | c) Die Einrichtung MUSS ermitteln, welche Rechte dem Cloud-Diensteanbieter oder Dritten an den dienstlichen Daten eingeräumt werden.<br>i) Die Einrichtung MUSS bewerten, ob diese Rechte mit der eigenen Sicherheitsrichtlinie vereinbar sind.<br>ii) Die Einrichtung MUSS insbesondere die Nutzungsbedingungen und die Datenschutzerklärung des Cloud-Diensteanbieters auswerten. | | |
| Vormals „MCD.2.1.07: Verschlüsselung der Daten“<br>Es ist zu ermitteln, wie die Daten vom Cloud-Anbieter verschlüsselt gespeichert werden. Es ist zu bewerten, ob die Verschlüsselung mit den Anforderungen aus den Ergebnissen der Datenkategorisierung und Risikoanalyse vereinbar sind.17 Ist die vom Cloud-Anbieter eingesetzte Verschlüsselung nicht geeignet, ist zu prüfen, ob Anforderungen an die Vertraulichkeit der Daten über eine | d) Die Einrichtung MUSS ermitteln, wie die dienstlichen Daten im externen Cloud-Dienst verschlüsselt gespeichert werden.<br>i) Die Einrichtung MUSS dann bewerten, ob die Verschlüsselung mit den Anforderungen aus den Ergebnissen der Datenkategorisierung vereinbar sind.<br>ii) Ist die vom Cloud-Diensteanbieter eingesetzte Verschlüsselung nicht geeignet, MUSS die Einrichtung prüfen, ob Anforderungen an die Vertraulichkeit der Daten über eine clientseitige Verschlüsselung erfüllt werden | | Die Anforderung, dienstliche Daten im externen Cloud-Dienst verschlüsselt zu speichern ergibt sich aus dem Abgleich identifizierter Risiken mit der Cloud-Strategie einer Einrichtung (siehe NCD.2.2.03 i). Daher wäre es zielführender, basierend auf den bereits ermittelten Ris ken zu entscheiden, ob in Erfahrung gebracht werden muss, wie die dienstlichen Daten im externen Cloud-Dienst verschlüsselt gespeichert werden. Existieren keine Risiken für die dienstlichen Daten, besteht keine Notwendigkeit die dienstlichen Daten verschlüsselt zu speichern und die hier beschriebene Aktivität ist obsolet. |

| Version 1.0 | RFC Beta V.1.0.5 | Hinweise | Bemerkungen |
|---|---|---|---|
| clientseitige Verschlüsselung erfüllt werden können. | können. | | |
| Vormals „MCD.2.1.08: Erforderliche Softwareinstallationen“<br>Es ist zu ermitteln, ob für die Mitnutzung auf Arbeitsplatzcomputern oder mobilen Endgeräten der IT-Anwender zusätzliche Softwareinstallationen erforderlich sind. Es ist zu bewerten, ob die hierfür einzuräumenden Zugriffs- und Ausführungsrechte mit der Informationssicherheitsrichtlinie der mitnutzenden Behörde vereinbar sind und inwiefern gesonderte Lizenzen für die Mitnutzung eingeholt werden müssen.<br>Ist ein Zugriff über mobile Endgeräte geplant, sind diese zentral zu verwalten. Die Vorgaben des Mindeststandards Mobile Device Management sind zu beachten. | e) Die Einrichtung MUSS ermitteln, ob für die Mitnutzung auf den eigenen Arbeitsplatzcomputern oder mobilen Endgeräten zusätzliche Softwareinstallationen erforderlich sind.<br>i) Die Einrichtung MUSS dann bewerten, ob die hierfür einzuräumenden Zugriffs- und Ausführungsrechte mit der eigenen IT-Sicherheitsrichtlinie vereinbar sind und inwiefern gesonderte Lizenzen für die Mitnutzung eingeholt werden müssen.<br>ii) Ist ein Zugriff über mobile Endgeräte geplant, MUSS die Einrichtung diese zentral verwalten. Die Vorgaben des Mindeststandards Mobile Device Management sind zu beachten.[xx]<br>[xx] Siehe Mindeststandard des BSI Mobile Device Management, (BSI 2017) | | |

**Von:** [redacted], 21C
**An:** GP Mindeststandards Bund
**Cc:** *IT-Sibe BAMF; [redacted], GL21; [redacted], GL22; *22B-RL; *22E-RL; CI4@bmi.bund.de
**Betreff:** AW: Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2.0
**Datum:** Montag, 11. Januar 2021 06:52:59
**Anlagen:** CDR_MST-NCD-RfC-Beta-1.0.5_Anmerkungen-BAMF-Abt2.docx

---

Sehr geehrte Damen und Herren,

vielen Dank für die Beteiligung am Konsultationsverfahren zu Version 2.0 des Mindeststandards zur Nutzung externer Cloud-Dienste.

Im Anhang finden Sie die Anmerkungen aus der IT-Abteilung des BAMF. Diese zielen u.a. darauf ab, einerseits Definitionen und Anwendungsgebiete zu schärfen und andererseits den mit der Einhaltung des Mindeststandards vergleichsweise (zu) hohen Sonderaufwand in Grenzen zu halten, zumal es sich bei externen Cloud-Diensten um keine Seltenheit in der Softwareentwicklung und -nutzung handelt und diese in IT-Sicherheitskonzepten wie andere Dienste auch bereits regulär berücksichtigt werden.

Zudem kam unabhängig von dem Konsultationsverfahren bei uns die Frage auf, ob/welche spezifischen Rahmenbedingungen für Sourcecode-Veröffentlichungen auf Github gelten.

Nach kurzer Recherche auf der BSI-Website bin ich auf Beispielprojekte wie z.B. Persosim von HJP und Botan 2.X des BSI gestoßen, wobei zu Letzterem ein umfangreiches Handbuch vorliegt ( https://botan.randombit.net/handbook/contents.html ), aber beispielhafte IT-Sicherheitskonzepte oder Sicherheitsprofile (wie es z.B. für SaaS gibt, https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Sicherheitsprofile/sicherheitsprofil_saas_node.html ) habe ich zu "Sourcecode-Veröffentlichungen auf Github" bislang nicht entdeckt. Falls Sie mir den hier geltenden (ggf. spezifischen) Rahmenbedingungen einen weiterführenden Hinweis geben können, wäre ich Ihnen sehr dankbar.

Für Rückfragen stehe ich gern zur Verfügung.

Freundliche Grüße
[redacted]
Referatsleiterin
Referat 21C Prozessentwicklung, IT-Architektur und Testmanagement
Bundesamt für Migration und Flüchtlinge, Frankenstr. 210, 90461 Nürnberg
Tel. 1: [redacted] Tel. 2 [redacted]
E-Mail: [redacted]@bamf.bund.de

-----Ursprüngliche Nachricht-----
Von: CI4@bmi.bund.de <CI4@bmi.bund.de>
Gesendet: Dienstag, 24. November 2020 15:55
An: [redacted]@bdbos.bmi.bund.de; [redacted]@polizei.bund.de; [redacted]@bva.bund.de; [redacted]@bsi.bund.de; [redacted]@bbk.bund.de; [redacted]@badv.bund.de; [redacted]@bakoev.bund.de; *IT-Sibe BAMF [redacted]@bamf.bund.de>; [redacted]@bbk.bund.de; [redacted]@bbr.bund.de; [redacted]@bescha.bund.de; [redacted]@bfv.bund.de; [redacted]@bib.bund.de; [redacted]@bisp.de; [redacted]@bka.bund.de; [redacted]@bkg.bund.de; [redacted]@bpb.bund.de;

[redacted]@polizei.bund.de; [redacted]@bsi.bund.de; [redacted]@hsbund.de;
[redacted]@destatis [redacted]@thw.bund.de;
[redacted]@zitis.bund.de; [redacted]@ZITiS.bund.de;
[redacted]@bmi.bund.de; [redacted]@bakoev.bund.de

Cc: CI4@bmi.bund.de; RegCI4@bmi.bund.de
Betreff: Mindeststandard zur Nutzung externer Cloud-Dienste, hier:
Konsultationsverfahren zum Major-Release Version 2.0

CI 4 - 17002/20#11

Liebe Kolleginnen und Kollegen,
im Zuge der Überarbeitung und Anpassung des Mindeststandards zur Nutzung externer Cloud-Dienste finden Sie im Anhang das Anschreiben des AL BL im BSI, Herrn Samsel, sowie den Entwurf zum Mindeststandard des BSI zur Nutzung externer Cloud-Dienste nach § 8Absatz 1 Satz 1 BSIG - RfC-Beta-Version 1.0.5 vom 17.11.2020. Die Änderungstabelle zum Mindeststandard ist der E-Mail ebenfalls beigefügt.

Bitte senden Sie Kommentierungen und Rückmeldungen bis zum 8. Januar 2021 per E-Mail an das Postfach mindeststandards@bsi.bund.de.

Mit freundlichen Grüßen
im Auftrag

[redacted]

Bundeministerium des Innern, für Bau und Heimat Referat CI 4
Cybersicherheit in der Bundesverwaltung
D-10557 Berlin, Alt-Moabit 140
Telefon: [redacted]
eMail: CI4@bmi.bund.de; Cc: [redacted]@bmi.bund.de
Internet: www.bmi.bund.de; www.cio.bund.de

-----Ursprüngliche Nachricht-----
Von: [redacted]@bsi.bund.de> Im Auftrag von GP Geschaeftszimmer_BL
Gesendet: Freitag, 20. November 2020 11:06
An: poststelle@bk.bund.de; poststelle@auswaertiges-amt.de; poststelle@bmi.bund.de; poststelle@bmf.bund.de; poststelle@bmjv.bund.de; poststelle@bmvg.bund.de; info@bmwi.bund.de; poststelle@bmas.bund.de; poststelle@bmel.bund.de; poststelle@bmfsfj.bund.de; poststelle@bmg.bund.de; poststelle@bmvi.bund.de; Poststelle@bmu.bund.de; information@bmbf.bund.de; poststelle@bmz.bund.de; bverfg@bundesverfassungsgericht.de; poststelle@bpra.bund.de; bundesrat@bundesrat.de; Poststelle@brh.bund.de; [redacted]@bundestag.de; Poststelle@bkm.bund.de; Poststelle@bfdi.bund.de; [redacted]@itzbund.de; [redacted]@jm nrw.de; GP AG-InfoSic [redacted]@bsi.bund.de>

Cc: GP Abteilung BL <abteilung-bl@bsi.bund.de>; GP Fachbereich BL 3 <fachbereich-bl3@bsi.bund.de>; GP Referat BL 35 <referat-bl35@bsi.bund.de>; GP Poststelle <poststelle@bsi.bund.de>; GP Stab 3 - Strategie und Leitungsunterstuetzung <stab3@bsi.bund.de>; GP Geschaeftszimmer_BL <geschaeftszimmer-bl@bsi.bund.de>

Betreff: [MST NCD] Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2.0

Sehr geehrte Damen und Herren,

anbei übersende ich Ihnen das Anschreiben sowie den Mindeststandard des BSI zur Nutzung externer Cloud-Dienste nach § 8 Absatz 1 Satz 1 BSIG - RfC-Beta-Version 1.0.5 vom 17.11.2020. Die Abgleichstabelle zum Mindeststandard ist der E-Mail ebenfalls beigefügt.

Mit freundlichen Grüßen
Im Auftrag

[redacted]

---

Geschäftszimmer BL
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 228 99 9582-[redacted]
Fax: +49 228 99 10 9582[redacted]
E-Mail: geschaeftszimmer-bl@bsi.bund.de
Internet: www.bsi.bund.de
www.bsi-fuer-buerger.de

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

# Mindeststandard des BSI zur Nutzung externer Cloud-Dienste

nach § 8 Absatz 1 Satz 1 BSIG – RfC-Beta-Version 1.0.5 vom 17.11.2020

# Änderungshistorie

| *Version* | *Datum* | *Beschreibung* |
|---|---|---|
| 1.0 | 24.04.2017 | Erstveröffentlichung |
| 1.0.1 | 13.07.2020 | RfC-Alpha-Version, Rohentwurf auf Basis der Delta-Dokumentation |
| 1.0.2 | 25.09.2020 | Prüfung, Überarbeitung und Freigabe durch Fachreferat |
| 1.0.3 | 29.09.2020 | RfC-Alpha-Version zur hausinternen Abstimmung |
| 1.0.4 | 09.11.2020 | Kommentare und Rückmeldungen aus der hausinternen Abstimmung eingearbeitet |
| 1.0.5 | 17.11.2020 | Ressorts erhalten Entwurf zur Kommentierung |

Tabelle 1: Versionsgeschichte des Mindeststandards. Eine ausführliche Änderungsübersicht zum Mindeststandard erhalten Sie unter: **Fehler! Linkreferenz ungültig.**~~https://www.bsi.bund.de/mindeststandards~~ (**Hinweis:** wird vor Release konkretisiert)

Bundesamt für Sicherheit in der Informationstechnik Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6262
E-Mail: mindeststandards@bsi.bund.de
Internet: https://www.bsi.bund.de

# Vorwort

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes auf der Grundlage des § 8 Abs. 1 BSIG. Als gesetzliche Vorgabe definieren Mindeststandards ein konkretes Mindestniveau für die Informationssicherheit. Der Umsetzungsplan Bund 2017 legt fest, dass die Mindeststandards des BSI auf Basis § 8 Abs. 1 BSIG zu beachten sind.[1] Die Definition erfolgt auf Basis der fachlichen Expertise des BSI in der Überzeugung, dass dieses Mindestniveau in der Bundesverwaltung nicht unterschritten werden darf. Der Mindeststandard richtet sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe)[2] und IT-Betriebspersonal.

IT-Systeme sind in der Regel komplex und in ihren individuellen Anwendungsbereichen durch die unterschiedlichsten (zusätzlichen) Rahmenbedingungen und Anforderungen gekennzeichnet. Daher können sich in der Praxis regelmäßig höhere Anforderungen an die Informationssicherheit ergeben, als sie in den Mindeststandards beschrieben werden. Aufbauend auf den Mindeststandards sind diese individuellen Anforderungen in der Planung, der Etablierung und im Betrieb der IT-Systeme zusätzlich zu berücksichtigen, um dem jeweiligen Bedarf an Informationssicherheit zu genügen. Die Vorgehensweise dazu beschreiben die IT-Grundschutz-Standards des BSI.

Zur Sicherstellung der Effektivität und Effizienz in der Erstellung und Betreuung von Mindeststandards arbeitet das BSI nach einer standardisierten Vorgehensweise. Zur Qualitätssicherung durchläuft jeder Mindeststandard mehrere Prüfzyklen einschließlich des Konsultationsverfahrens mit der Bundesverwaltung.[3] Über die Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich jede Stelle des Bundes auch bei der Erschließung fachlicher Themenfelder für neue Mindeststandards einbringen oder im Hinblick auf Änderungsbedarf für bestehende Mindeststandards Kontakt mit dem BSI aufnehmen. Einhergehend mit der Erarbeitung von Mindeststandards berät das BSI die Stellen des Bundes[4] auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Vgl. Umsetzungsplan Bund 2017 (BMI 2017), S. 4
[2] Analog „Informationssicherheitsbeauftragter (ISB)“
[3] Siehe FAQ zu den Mindeststandards (BSI 2020)
[4] Zur besseren Lesbarkeit wird im weiteren Verlauf für „Stelle des Bundes“ der Begriff „Einrichtung“ verwendet.

# Inhalt



Feldfunktion geändert

# 1 Beschreibung

Dieser Mindeststandard setzt Sicherheitsanforderungen an die Nutzung externer Cloud-Dienste. Die Erfüllung der im Mindeststandard vorgegebenen Sicherheitsanforderungen ist für ein angemessenes IT-Sicherheitsniveau notwendig, aber in der Regel nicht hinreichend. Unter Berücksichtigung des individuellen Schutzbedarfs muss die Festlegung und Umsetzung eventuell zusätzlich erforderlicher Sicherheitsanforderungen erfolgen. Er richtet sich hinsichtlich seiner Umsetzung an IT-Sicherheitsbeauftragte, IT-Betriebs- und Fachverantwortliche.[5]

## 1.1 Begriffsbestimmung und Abgrenzung

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Insbesondere werden dabei Infrastrukturen, Plattformen und Software angeboten, die Spannbreite der angebotenen Cloud-Dienste umfasst darüber hinaus jedoch das komplette Spektrum der Informationstechnik.[6]

Externe Cloud-Dienste im Sinne dieses Mindeststandards sind im Rahmen von Cloud Computing angebotene Dienstleistungen, die über Netze und Anbieter der Wirtschaft außerhalb der öffentlichen Verwaltung des Bundes und der Länder erbracht werden.[7]

Als Nutzung ist eine Verarbeitung von dienstlichen Daten[8] durch einen externen Cloud-Dienst zu verstehen, der durch die Einrichtung selbst oder gemeinsam mit anderen beauftragt wird. Werden externe Cloud-Dienste durch Benutzer[9] einer Einrichtung lediglich mitgenutzt, regelt Kapitel 2.5 den Umgang mit dienstlichen Daten in diesen Fällen entsprechend. Von einer Mitnutzung wird insbesondere ausgegangen, wenn die Einrichtung den externen Cloud-Dienst~~en~~ nicht beauftragt hat.

Werden keine dienstlichen Daten verarbeitet, können die Regelungen des Mindeststandards trotzdem angewendet werden (siehe NCD.2.1.03, Buchstabe e)).

## 1.2 Modalverben

In Anlehnung an den IT-Grundschutz[10] werden die Sicherheitsanforderungen mit den Modalverben MUSS und SOLLTE sowie den zugehörigen Verneinungen formuliert. Darüber hinaus wird das Modalverb KANN für ausgewählte Prüfaspekte verwendet. Die hier genutzte Definition basiert auf RFC 2119[11] und DIN 820-2: 2018[12].

**MUSS / DARF NUR**

bedeutet, dass diese Anforderung zwingend zu erfüllen ist. Das von der Nichtumsetzung ausgehende Risiko kann nicht im Rahmen einer Risikoanalyse akzeptiert werden.

**DARF NICHT / DARF KEIN**

**Kommentiert [FH21]:** Sofern der Cloud-Dienst des privatwirtschaftlichen Anbieters als „Blackbox" innerhalb der Netze der öffentlichen Verwaltung (im Sinne einer Appliance / Disconnected-Modes) angeboten/betrieben wird, könnte dieser ebenfalls als „externer Cloud-Dienst" gelten (insbesondere, wenn eine Anbindung dieses Dienstes ans Internet erfolgt). M.E. ist die Verortung des Cloud-Dienstes nicht (alleine) ausschlaggebend.

**Kommentiert [h2]:** Sofern unter den zu verarbeitenden dienstlichen Daten auch personenbezogene Daten sind, ist ggf. ein Fall der Auftragsverarbeitung gemäß Artikel 28 DSGVO anzunehmen.
Der Zusammenhang zur DSGVO sollte m.E. hier deutlicher herausgestellt oder, falls keiner besteht, bewusst davon abgegrenzt werden.

[5] Rollen nach IT-Grundschutz-Kompendium, (BSI 2020b), S.31
[6] Definition nach Fehler! Linkreferenz ungültig.~~https://www.bsi.bund.de/cloud~~
[7] Hinweis: IT-Dienstleistungen der „Bundescloud" fallen somit nicht unter diese Bestimmung.
[8] Dienstlich sind alle Daten, die im Rahmen der dienstlichen Tätigkeit erhoben und verarbeitet werden. Zu dienstlichen Daten gehören grundsätzlich auch personenbezogene Daten. Darunter fallen jedoch nicht solche personenbezogenen Daten (wie Stammdaten, Nutzungsdaten), die für die Registrierung und Nutzung des Dienstes vom Cloud-Diensteanbieter erhoben oder verarbeitet werden.
[9] Analog Rolle „Benutzer" nach IT-Grundschutz-Kompendium, (BSI 2020b), S.31
[10] Vgl. BSI-Standard 200-2 (BSI 2017), S. 18
[11] Vgl. Key words for use in RFCs (IETF 1997)
[12] Vgl. DIN-820-2: Gestaltung von Dokumenten (DIN 2018)

bedeutet, dass etwas zwingend zu unterlassen ist. Das durch die Umsetzung entstehende Risiko kann nicht im Rahmen einer Risikoanalyse akzeptiert werden.

**SOLLTE**

bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

**SOLLTE NICHT / SOLLTE KEIN**

bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

**KANN**

bedeutet, dass die Umsetzung / Nicht-Umsetzung optional ist und ohne Angabe von Gründen unterbleiben kann.

# 2 Sicherheitsanforderungen

Nachfolgende Sicherheitsanforderungen adressieren die Informationssicherheit entlang des gesamten Lebenszyklus und setzen auf den IT-Grundschutz-Baustein OPS.2.2 *Cloud-Nutzung*[13] auf.

## 2.1 Planungsphase

Grundlage der Informationssicherheit im Bereich Cloud Computing bilden nach dem IT-Grundschutz-Baustein OPS.2.2: *Cloud-Nutzung*

- die Cloud-Nutzungs-Strategie
- die darauf basierende Sicherheitsrichtlinie sowie
- das jeweilige Sicherheitskonzept für den externen Cloud-Dienst.

Die nachfolgenden Sicherheitsanforderungen adressieren diese Dokumente entsprechend.

**NCD.2.1.01 Cloud-Nutzungs-Strategie**

a) Die Einrichtung MUSS prüfen, ob der externe Cloud-Dienst grundsätzlich mit den in der Cloud-Nutzungs-Strategie definierten Zielen, Chancen und Risiken vereinbar ist.[14]

b) Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn Ziele, Chancen und Risiken der Cloud-Nutzungs-Strategie angemessen berücksichtigt werden können.

**NCD.2.1.02 Sicherheitsrichtlinie externe Cloud-Dienste**

a) Die Einrichtung MUSS eine Sicherheitsrichtlinie für externe Cloud-Dienste nach OPS.2.2.A2 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*[15] erstellen.

b) Die Einrichtung MUSS in dieser Sicherheitsrichtlinie mindestens die Umsetzung und Einhaltung der Basiskriterien nach dem Kriterienkatalog Cloud Computing (C5) als spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter festlegen.[16]

c) Die Einrichtung MUSS die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragen bei der Erstellung der Sicherheitsrichtlinie beteiligen.

**NCD.2.1.03 Sicherheitskonzept für den externen Cloud-Dienst**

a) Die Einrichtung MUSS ein Sicherheitskonzept für den externen Cloud-Dienst nach OPS.2.2.A7 *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung* erstellen.

b) Die Einrichtung MUSS in dem Sicherheitskonzept die aktuellen Veröffentlichungen des BSI zu Cloud-Sicherheit berücksichtigen.[17]

c) Die Einrichtung MUSS die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragen bei der Erstellung des Sicherheitskonzeptes beteiligen.

d) Die Einrichtung MUSS eine Datenkategorisierung durchführen, in der sämtliche dienstliche Daten identifiziert werden, die künftig in dem externen Cloud-Dienst verarbeitet werden sollen.

[13] IT-Grundschutz-Kompendium, (BSI 2020b), OPS.2.2: *Cloud-Nutzung*
[14] Hinweis: OPS.2.2.A1 *Erstellung einer Cloud-Nutzungs-Strategie* sieht die Erstellung einer Cloud-Nutzungs-Strategie vor. In dieser erfasst die Einrichtung ihre Ziele, Chancen und Risiken, die sie mit einer Cloud-Nutzung generell verbindet. Die Cloud-Nutzungs-Strategie nimmt daher eine zentrale Rolle für die Einrichtung ein. Sie wird benötigt, um die beabsichtigte Nutzung eines konkreten externen Cloud-Dienstes bewerten zu können.
[15] IT-Grundschutz-Kompendium, (BSI 2020b), OPS.2.2: *Cloud-Nutzung*
[16] Kriterienkatalog Cloud Computing (C5), (BSI 2020a), S.1ff.
[17] Siehe Veröffentlichungen unter Fehler! Linkreferenz ungültig.~~https://www.bsi.bund.de/cloud~~

**Kommentiert [h3]:** Der gesamte Abschnitt 2 sollte m.E. noch klarer zwischen Nutzung und Mitnutzung unterscheiden.
Bspw.:
Gilt wirklich nur Kapitel 2.5 für Mitnutzung-Dienste und gelten die Kapitel 2.1-2.4 nur für Nutzung-Dienste? Wenn ja, dann sollte das am Anfang von Abschnitt 2 klargestellt werden. Wenn Teile der Kapitel 2.1-2.4 auch für Mitnutzung-Dienste gelten, wäre das kenntlich zu machen.

Dass Kapitel 2.2 nur für Nutzung-Dienste gilt (weil diese mit Beschaffung und Beauftragung verbunden sind), leuchtet ein. Aber eine Planungsphase sollte es ggf. auch bei Mitnutzung-Diensten geben, wobei dabei vermutlich nicht das ganze Kapitel 2.1 zu beachten ist.

Grundsätzlich sei hier angemerkt, dass es sehr schlanke Mitnutzung-Möglichkeiten gibt, z.B. Cloud-Dienste, die im Internet leicht verfügbar und oftmals auch als freeware (ggf. mit Apache Lizenz, mit AGG, aber nicht unbedingt mit Vertrag – was ja dann keine Nutzung, sondern nur Mitnutzung ist) angeboten werden. Hierfür die gesamten Aufgaben aus Kap. 2.1 ff. abzuarbeiten, wäre ein unverhältnismäßiger und auch nicht erforderlicher Aufwand. Es sollte also insbesondere bei OSS darauf geachtet werden, dass Sicherheitsmaßnahmen ausreichend umgesetzt, aber keine übermäßigen konzeptionellen Aufwände für jeden kleinen Individualfall der Cloud-(Mit)Nutzung betrieben werden müssen.

Außerdem gibt es sicherlich auch schlanke Nutzung-Dienste. Hier ein Beispiel (mit der hypothetischen Annahme, dass es solch einen Service noch nicht als geeignete OSS gibt und folgende neue Beauftragung erfolgt): Eine Behörde beauftragt eine Firma mit der Entwicklung eines Wechselkursrechners, der an dem offiziellen Wechselkurs der betroffenen Nationalbanken orientiert ist. Die Firma entwickelt den Wechselkursrechner und bietet den Service in Form eines Cloud-Dienst eines externen Anbieters an. Die Behörde nimmt die Leistung auf Basis des mit der Firma geschlossenen Vertrages an. Die Behörde nutzt den Wechselkursrechner, indem sie Zahlenbeträge und d ... [1]

**Kommentiert [h4]:** Es ist zu hinterfragen, ob diese Strategie zwingend erforderlich ist.
Das Erfordernis gemäß OPS.2.2 basiert auf der darin geäußerten Annahme, dass Cloud-Nutzung eine strategische Entscheidung ist.
Gilt das so pauschal?
Es könnte zunehmend Services geben, die nur noch (effizient) in Cloud-Technologien zur Verfügung gestellt werden bzw. für die eine andere Bereitstellung einen unverhältnismäßigen und auch sonst nicht gerechtfertigten Aufwand erfordern würde.
Wenn heutzutage Cloud-Dienste immer üblicher werden, warum sollte man speziell für jeden Einzelnen eine dedizierte Cloud-Strategie haben müssen? Schließlich ist es ja auch nicht üblich eine „Strategie" für die Nutzung von Wasser und Strom zu haben, sondern man behandelt solche Themen in Betriebs- und Sicherheitskonzepten, i.d.R. ohne strategische Ziele damit zu verfolgen.
Wenn allerdings generell eine IT-Strategie in der Behörde erstellt wird, könnte darin natürlich ein Abschnitt bzgl. Cloud-Nutzung enthalten sein.

e) Kommt die Einrichtung zu dem Ergebnis, dass in dem externen Cloud-Dienst keine dienstlichen Daten verarbeitet werden, handelt es sich nicht um eine Nutzung oder Mitnutzung externer Cloud-Dienste im Sinne dieses Mindeststandards. In diesem Fällen KANN die Einrichtung die Sicherheitsanforderungen des Mindeststandards umsetzen.

Kommentiert [h5]: Da dieser Punkt zu dem letzten Satz in Kapitel 1.1 redundant ist, kann er entfallen.

f) Die Einrichtung MUSS für die identifizierten dienstlichen Daten Geheim- und Datenschutzaspekte[18] sowie Personen- und Dienstgeheimnisse ermitteln.

g) Die Einrichtung MUSS die identifizierten dienstlichen Daten den nachfolgenden Kategorien zuordnen:

- Kategorie 1 = Privat- und Dienstgeheimnisse gemäß §§ 203 und 353b StGB
- Kategorie 2 = personenbezogene Daten gemäß § 3 Absatz 1 BDSG
- Kategorie 3 = Verschlusssachen gemäß Verschlusssachenanweisung - VSA[19]
- Kategorie 4 = sonstige Daten (weder Kategorie 1, noch 2, noch 3)

h) Die Einrichtung KANN die identifizierten dienstlichen Daten den Kategorien 1, 2 und~~oder~~ 3 gleichzeitig zuordnen.

i) Die Einrichtung MUSS Risiken, die aus der künftigen Nutzung des externen Cloud-Dienstes entstehen können, umfassend ermitteln.[20]

i) Die Einrichtung MUSS die ermittelten Risiken mit denen in der eigenen Cloud-Nutzungs-Strategie (siehe NCD.2.1.01) festgelegten Richtlinien der Risikobewertung abgleichen und bewerten.

ii) Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn die ermittelten Risiken gemäß der in der Cloud-Nutzungs-Strategie genannten Richtlinien zur Risikobewertung wirksam vermieden oder hinreichend reduziert oder getragen werden können.

**NCD.2.1.04 Notfall- und Kontinuitätsmanagement**

Mit Notfall- bzw. Kontinuitätsmanagement ist gemäß BSI-Standard 100-4[21] ein Managementsystem zur Aufrechterhaltung einer definierten Arbeitsfähigkeit einer Einrichtung gemeint und umfasst sowohl präventive als auch reaktive Maßnahmen auf Notfälle und Krisensituationen. Es gilt im weiteren die Begrifflichkeit des BSI-Standards 100-4[22].

a) Die Einrichtung MUSS prüfen, ob sie in Notfällen und Krisensituationen weiter auf den externen Cloud-Dienst zugreifen können muss. [23]

b) Die Einrichtung MUSS bewerten, welche Bedeutung der externe Cloud-Dienst in Notfällen einnehmen würde.[24]

[18] Hinsichtlich Datenschutzaspekte siehe insbesondere (AKTM 2011), S.1ff.
[19] Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), (BMI 2018)
[20] Hinweis: Bei dieser Prüfung geht es um eine anbieterunabhängige Prüfung. Es soll in diesem Zusammenhang geklärt werden, ob das beabsichtigte Cloud-Szenario mit der Cloud-Nutzung-Strategie vereinbar ist (z.B. Können die eigenen rechtlichen und organisatorischen Rahmenbedingungen überhaupt erfüllt werden?)
[21] BSI-Standard 100-4 – Notfallmanagement, (BSI 2008), S.1ff.
[22] BSI-Standard 100-4 – Notfallmanagement, (BSI 2008), S.1ff.
[23] Hinweis: Leitfragen für diese Prüfung können sein: Wird der Cloud-Dienst für einen, im Notfallmanagement als zeitkritisch bewerteten Geschäftsprozess (bzw. Fachaufgabe) genutzt? Dient der Cloud-Dienst zur Etablierung und Aufrechterhaltung eines Notbetriebs? Ist der Cloud-Dienst für die Bewältigung eines Notfalls relevant?
[24] Hinweis: Leitfragen für diese Prüfung können sein: Wie zeitkritisch sind die Geschäftsprozesse (bzw. Fachaufgaben), die den Cloud-Dienst in einem Notfall oder einer Krise benötigen? Zu welchem Grad wird der Cloud-Dienst in einem Notbetrieb benötigt?

c) Die Einrichtung MUSS den zuständigen Notfallbeauftragten entsprechend einbinden. Dieser MUSS prüfen, ob die Prävention vor bzw. die Reaktion auf Notfälle oder Krisen durch die Cloud-Nutzung geändert werden muss. Die Einrichtung MUSS diese Änderungen vor der Cloud-Nutzung umsetzen.

## 2.2 Beschaffungsphase

Ziel des Beschaffungsprozesses, für den die Vorgaben des Vergaberechts einschlägig sind, ist die Auswahl eines geeigneten Cloud-Diensteanbieters.

**NCD.2.2.01 Umsetzung der Sicherheitsanforderungen**

a) Die Einrichtung MUSS vor Vertragsabschluss überprüfen, ob die in ihrer Sicherheitsrichtlinie festgelegten Sicherheitsanforderungen (siehe NCD.2.1.02, Buchstabe a)) vom Cloud-Diensteanbieter erfüllt werden können.[25]

b) Die Einrichtung MUSS diese Sicherheitsanforderungen bereits in der Leistungsbeschreibung des externen Cloud-Dienstes einfordern.

c) Die Einrichtung MUSS die Angaben und Nachweise des Cloud-Diensteanbieters zu Buchstabe a) hinsichtlich Inhalt, Aussagekraft, Nachvollziehbarkeit, Aktualität, nachteiliger Regelungen sowie Mitwirkungspflichten und Maßnahmen auswerten. Dazu SOLLTE der „*Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5*“[26] verwendet werden.

d) Die Einrichtung MUSS sich die regelmäßige Vorlage von Sicherheitsnachweisen vom Cloud-Diensteanbieter zusichern lassen.

e) Diese Sicherheitsnachweise SOLLTEN

- die angemessene und wirksame Umsetzung der Basiskriterien nach C5[27],
- die aktuelle Dokumentation der Systembeschreibung[28],
- die Aktualität von vertraglich zugesicherten Zertifizierungen sowie
- die ordnungsgemäße Durchführung von Datensicherungen und erprobten Rücksicherungen

umfassen und durch die regelmäßige Bereitstellung des aktuellen Prüfberichtes nach C5 erbracht werden. Andere Nachweise DARF die Einrichtung NUR in begründeten Einzelfallentscheidungen zulassen.

f) Die Einrichtung MUSS die Sicherheitsnachweise des Cloud-Diensteanbieters auswerten. Insbesondere DÜRFEN Prüfberichte und Nachweise über den Nutzungszeitraum KEINE zeitlichen Lücken enthalten.

g) Die Einrichtung MUSS sich die Einhaltung vorgesehener und vereinbarter Prozesse sowie die Durchführung von Audits, Sicherheitsprüfungen, Penetrationstests und Schwachstellenanalysen durch den Cloud-Diensteanbieter vertraglich zusichern lassen.

h) Die Einrichtung MUSS ermittelte Risiken, die nicht bereits durch Basiskriterien nach C5 abgedeckt sind, über zusätzliche Anforderungen abdecken oder diese Risiken transferieren oder diese Risiken tragen.

[25] Hinweis: Liegt ein Prüfbericht nach C5 vor, können diese Informationen daraus entnommen werden.

[26] Hinweis: Der Auswertungsleitfaden gibt eine Struktur vor, welche die Einrichtung darin unterstützt, einen C5-Bericht systematisch auszuwerten. Dies beinhaltet, die Sicherheitsmaßnahmen des Cloud-Diensteanbieters (und die zugehörigen Prüfergebnisse) aufzunehmen, die eigenen Nutzerkontrollen für die Nutzung einzurichten und hierdurch das mit der Cloud-Nutzung verbundene Risiko einzuschätzen und steuern zu können. Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“, (BSI 2020c), **Fehler! Linkreferenz ungültig.**~~https://www.bsi.bund.de~~

[27] Hinweis: Die im C5 festgelegten Übergangsfristen für neue Versionen sind zu beachten.

[28] Hinweis: Im Falle einer „direkten Prüfung“ (vgl. C5, (BSI 2020a), Kap. 4.4.5, S.16f.) enthält der Bericht keine Systembeschreibung vom Anbieter, sondern eine vom Prüfer im Rahmen der Prüfung erhobene Beschreibung mit vergleichbarem Inhalt, die im Rahmen der Tätigkeiten dieses Mindeststandards herangezogen werden kann.

i) Die Einrichtung MUSS prüfen, ob sie weiteren Anforderungen (z. B. aus Gesetzen, Verordnungen, Beschlüssen oder anderen Quellen) unterliegt, die hinsichtlich der Cloud-Nutzung relevant sind. Diese Anforderungen MUSS die Einrichtung einhalten. Sie werden im Übrigen durch diesen Mindeststandard nicht berührt.

ii) Für die zusätzlichen Anforderungen MUSS die Einrichtung vereinbaren, dass regelmäßig geeignete Nachweise ihrer angemessenen und wirksamen Umsetzung vorgelegt werden.

i) Die Einrichtung SOLLTE sich eigene Prüfrechte vertraglich zusichern lassen.

i) Aufgrund der Ergebnisse aus der Datenkategorisierung und Risikoanalyse KANN die Einrichtung in begründeten Fällen auf eigene Prüfrechte verzichten, soweit Rechtsvorschriften nicht entgegenstehen.

ii) Die Einrichtung MUSS darauf achten, dass die Prüfrechte so ausgestaltet sind, dass die Einrichtung ihre gesetzlichen Anforderungen erfüllt.

iii) Die Einrichtung MUSS die Prüfrechte so ausgestalten, dass sie nach Art und Umfang einen Nachweis des Schutzniveaus ermöglichen und die Prüfung durch die Einrichtung selbst oder durch Dritte in ihrem Auftrag (z. B. andere Stellen, externe IT-Revisoren oder Wirtschaftsprüfer) durchgeführt werden kann.

iv) Sofern der Cloud-Diensteanbieter keinen Prüfbericht nach C5 vorlegen kann, MUSS die Einrichtung dazu berechtigt sein, die Prüfung nach C5 durch Dritte selbst beauftragen zu können.

**NCD.2.2.02 Umgang mit Unterauftragnehmern und anderen externen Dritten vertraglich zusichern**

a) Die Einrichtung MUSS sich die Beteiligung von relevanten Unterauftragnehmern und anderen externen Dritten vom Cloud-Diensteanbieter vollständig in Art und Umfang benennen lassen. Die Entscheidung, welcher Unterauftragnehmer hier zu nennen ist, MUSS gemäß den Vorgaben des C5[29] erfolgen.

b) Die Einrichtung MUSS mit dem Cloud-Diensteanbieter vereinbaren, dass beabsichtigte Änderungen hierüber unverzüglich schriftlich oder per E-Mail mitgeteilt werden.

c) Diese Mitteilungen KÖNNEN über Internetportale bereitgestellt werden, wenn dadurch die Anforderungen gleichwertig erfüllt sind (z. B. durch Push-Benachrichtigungen).

d) Falls Unterauftragnehmer wesentliche Teile[30] zur Entwicklung oder zum Betrieb des Cloud-Dienstes beitragen, MUSS sich die Einrichtung vom Cloud-Diensteanbieter zusichern lassen, dass

- Unterauftragnehmer ebenfalls die vertraglich festgelegten Vorgaben erfüllen und
- zugesicherte Prüfrechte sich auch auf Unterauftragnehmer beziehen.

**NCD.2.2.03 Gerichtsbarkeit vertraglich zusichern**

a) Die Einrichtung SOLLTE zur Absicherung der Verfügbarkeit als Teil der Informationssicherheit Vereinbarungen ausschließlich nach deutschem Recht und deutschem Gerichtsstand und ohne obligatorisch vorab zu betreibende Schlichtungsverfahren abschließen.

b) Die Einrichtung MUSS berücksichtigen, dass bei gegebenenfalls notwendigem Rechtsschutz beziehungsweise Eilrechtsschutz Zeitverluste eintreten können, insbesondere durch eine Einarbeitung in fremde Rechtsordnungen oder ein Auftreten vor entfernt gelegenen Gerichten.

c) Die Einrichtung MUSS sicherstellen, dass sie handlungsfähig bleibt und ihre Forderungen effektiv durchsetzen kann.

[29] Kriterienkatalog Cloud Computing (C5), (BSI 2020a), Kap. 4.4.5, S.18f.
[30] Hinweis: Hinsichtlich Bestimmung „wesentlicher Teile“ siehe C5, (BSI 2020a), S.91

**NCD.2.2.04 Lokation vertraglich zusichern**

a) Die Einrichtung MUSS sämtliche Lokationen, an denen dienstliche Daten verarbeitet werden, vertraglich festlegen.

b) Die Einrichtung MUSS prüfen, ob die dienstlichen Daten an den vertraglich zugesicherten Lokationen verarbeitet werden dürfen. Dabei MUSS die Einrichtung die Ergebnisse der Datenkategorisierung und Risikoanalyse sowie der möglichen Gefahr eines fremdstaatlichen Zugriffs (z. B. durch Nachrichtendienste oder Ermittlungsbehörden) bewerten.

**NCD.2.2.05 Offenbarungspflichten und Ermittlungsbefugnisse vertraglich zusichern**

a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter zusichern lassen, dass Daten nicht in den Bereich fremdstaatlicher Offenbarungspflichten und Ermittlungsbefugnisse gelangen.[31]

b) Die Einrichtung MUSS die Pflichten des Cloud-Diensteanbieters, sicherheitsrelevante Vorfälle (sowie ggf. andere Vorfälle) gegenüber der Einrichtung zu melden, vertraglich regeln.

i) Die Einrichtung MUSS bei Vertragsstrafen und Haftungsfragen auf ein angemessenes Verhältnis zum ermittelten Schutzbedarf achten.

ii) Bei der Festlegung sind die aus rechtlicher Sicht zulässigen Grenzen zu berücksichtigen. Die Einrichtung SOLLTE bei der Ansetzung von Vertragsstrafen 5% des Auftragsvolumens nicht unterschreiten.

**NCD.2.2.06 Beendigung des Vertragsverhältnisses regeln**

a) Die Einrichtung MUSS Kündigungsfristen dem Einsatzszenario angemessen festlegen.

b) Soweit rechtlich möglich, MUSS die Einrichtung kurzfristige einseitige Kündigungs- oder Zurückbehaltungsrechte an den Leistungen zu Lasten der Einrichtung ausschließen.

**NCD.2.2.07 Datenrückgabe und Datenlöschung beim Cloud-Diensteanbieter vertraglich zusichern**

a) Die Einrichtung MUSS die Rückgabe der Daten regeln (Format, Datenträger, Protokolle, usw.).

b) Die Einrichtung MUSS berücksichtigen, dass die Maßnahmen zur Datenlöschung dem ermittelten Schutzbedarf entsprechen.

## 2.3 Einsatzphase

Mindestanforderungen an den Einsatz von externen Cloud-Diensten regeln, wie die vertraglich zugesicherten Leistungen überwacht und überprüft werden.

**NCD.2.3.01 ISMS einbinden**

a) Die Einrichtung MUSS den externen Cloud-Dienst in ihr eigenes Informationssicherheitsmanagementsystem (ISMS) einbinden.

b) Die Einrichtung MUSS die im C5-Bericht genannten korrespondierenden Kontrollen des Cloud-Dienstes bei sich einrichten. Die Einrichtung SOLLTE bei der Einbindung in das eigene ISMS zusätzlich die korrespondierenden Kriterien des C5[32] berücksichtigen.

**NCD.2.3.02 Sicherheitsnachweise prüfen**

[31] Auf die geltenden Regelungen zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden wird in diesem Zusammenhang entsprechend verwiesen. (BMI 2014), S.1

[32] Hinweis: Der C5 führt mit Version 2020 Mitwirkungspflichten des Kunden als korrespondierende Kriterien ein. Die Umsetzung liegt im Verantwortungsbereich des Kunden und ist entscheidend für die Aufrechterhaltung der Informationssicherheit eines Cloud-Dienstes. Siehe C5, (BSI 2020a), S.9

a) Die Einrichtung MUSS die Nachweise und sonstige Berichte des Cloud-Diensteanbieters auswerten.[33]

i) Diese DÜRFEN über den Nutzungszeitraum KEINE zeitlichen Lücken enthalten.

ii) Ergeben sich aus der Auswertung Unklarheiten, MUSS die Einrichtung diesen nachgehen.

b) Die Einrichtung MUSS prüfen, ob festgestellten Unklarheiten durch Wahrnehmung der zugesicherten Prüf- und Kontrollrechte nachzugehen ist.

**NCD.2.3.03 Leistungsfähigkeit prüfen**

a) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten ihrer eigenen IT-Infrastruktur, wie Performance der Netzanbindung und -verbindungen, beurteilen.

b) Die Einrichtung MUSS auf Abweichungen reagieren und die eigene IT-Infrastruktur und Netzanbindung den Ergebnissen der Überprüfung anpassen.

c) Die Einrichtung MUSS mindestens jährlich die Leistungsfähigkeiten des Cloud-Diensteanbieters, wie Performance des Cloud-Services und die Netzverbindung zum Cloud-Diensteanbieter, beurteilen.[34]

**NCD.2.3.04 Informationspflichten nachhalten**

a) Die Einrichtung MUSS nachhalten, dass der Cloud-Diensteanbieter seinen vertraglichen Informationspflichten stets nachkommt. Dies gilt insbesondere bei

i) einer Eingliederung in ein anderes Unternehmen oder einen anderen Konzern oder in sonstigen Fällen des Wechsels des wirtschaftlichen Eigentums an ihn,

ii) einem Austausch von Unterauftragnehmern oder Dritten.

b) Die Einrichtung MUSS Meldungen des Cloud-Diensteanbieters über relevante Störungen und Cyber-Angriffe dokumentieren und gemäß den vereinbarten Mitwirkungspflichten nach NCD.2.2.01, Buchstabe c) reagieren.

**NCD.2.3.05 Zwei-Faktor-Authentifizierungen aktivieren**

a) Bietet der externe Cloud-Dienst eine Zwei-Faktor-Authentifizierung als Identitätsnachweis seiner Benutzer (Log-in) an, SOLLTE die Einrichtung diese nutzen.

## 2.4 Beendigungsphase

**Mindestanforderungen an die Beendigung der Cloud-Nutzung adressieren die geordnete Beendigung des Vertragsverhältnisses.[35]**

**NCD.2.4.01 Datenrückgabe durchführen**

a) Die Einrichtung MUSS prüfen, ob der Cloud-Diensteanbieter alle Daten in der vereinbarten Form zurück übergeben hat.

b) Die Einrichtung MUSS die Übergabe dokumentieren.

**NCD.2.4.02 Datenlöschung bestätigen**

a) Die Einrichtung MUSS sich vom Cloud-Diensteanbieter die gemäß NCD2.2.07 erfolgte Löschung aller Daten, einschließlich vorhandener Datensicherungen, bestätigen lassen.

b) Die Bestätigung nach Buchstabe a) MUSS auch Daten und Datensicherungen bei möglichen Unterauftragnehmern und anderen externen Dritten umfassen.

c) Die Einrichtung MUSS die Datenlöschung dokumentieren.

**Kommentiert [h6]:** Ggf. hier noch klarstellen, dass neben den Nutzdaten auch Protokoll-/Transaktionsdaten zu löschen sind, sofern so vorgesehen.

[33] Siehe „Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5“, (BSI 2020c), Fehler! Linkreferenz ungültig ~~https://www.bsi.bund.de~~

[34] Hinweis: Viele Cloud-Diensteanbieter stellen diese Information kontinuierlich bereit, so dass diese Überprüfung als kontinuierliches Monitoring ausgestaltet werden kann. Mit dieser Anforderung ist gemeint, dass die vom Cloud-Diensteanbieter gelieferten oder von der Einrichtung erhobenen Daten zur Leistungsfähigkeit regelmäßig (mindestens jährlich) zu einer Beurteilung der Leistungsfähigkeit verdichtet und bewertet werden.

[35] Siehe OPS.2.2.A14 *Geordnete Beendigung eines Cloud-Nutzungsverhältnisses*, (BSI 2020b), S.1ff

## 2.5 Sicherheitsanforderungen bei einer Mitnutzung

Nehmen Benutzer einer Einrichtung einen externen Cloud-Dienst in Anspruch, ohne dass zwischen dieser Einrichtung und Cloud-Diensteanbieter ein Vertragsverhältnis besteht, geht dieser Mindeststandard von einer sog. Mitnutzung aus.[36] Für diesen Anwendungsfall regeln die nachfolgenden Sicherheitsanforderungen das Mindestsicherheitsniveau.

**NCD.2.5.01 Mitnutzung von externen Cloud-Diensten**

a) Die Einrichtung MUSS die Sicherheitsanforderungen nach NCD.2.1.03, Buchstaben d) bis i) umsetzen und einhalten.

b) Die Einrichtung MUSS ermitteln, an welchen Lokationen dienstliche Daten verarbeitet werden.

i) Die Einrichtung MUSS dann bewerten, ob aus ihrer Sicht die dienstlichen Daten an diesen Lokationen verarbeitet werden dürfen.

ii) Für diese Bewertung MUSS die Einrichtung insbesondere die Ergebnisse der Datenkategorisierung heranziehen.

c) Die Einrichtung MUSS ermitteln, welche Rechte dem Cloud-Diensteanbieter oder Dritten an den dienstlichen Daten eingeräumt werden.

i) Die Einrichtung MUSS bewerten, ob diese Rechte mit der eigenen Sicherheitsrichtlinie vereinbar sind.

ii) Die Einrichtung MUSS insbesondere die Nutzungsbedingungen und die Datenschutzerklärung des Cloud-Diensteanbieters auswerten.

d) Die Einrichtung MUSS ermitteln, wie die dienstlichen Daten im externen Cloud-Dienst verschlüsselt gespeichert werden.

i) Die Einrichtung MUSS dann bewerten, ob die Verschlüsselung mit den Anforderungen aus den Ergebnissen der Datenkategorisierung vereinbar sind.

ii) Ist die vom Cloud-Diensteanbieter eingesetzte Verschlüsselung nicht geeignet, MUSS die Einrichtung prüfen, ob Anforderungen an die Vertraulichkeit der Daten über eine clientseitige Verschlüsselung erfüllt werden können.

e) Die Einrichtung MUSS ermitteln, ob für die Mitnutzung auf den eigenen Arbeitsplatzcomputern oder mobilen Endgeräten zusätzliche Softwareinstallationen erforderlich sind.

i) Die Einrichtung MUSS dann bewerten, ob die hierfür einzuräumenden Zugriffs- und Ausführungsrechte mit der eigenen IT-Sicherheitsrichtlinie vereinbar sind und inwiefern gesonderte Lizenzen für die Mitnutzung eingeholt werden müssen.

ii) Ist ein Zugriff über mobile Endgeräte geplant, MUSS die Einrichtung diese zentral verwalten. Die Vorgaben des Mindeststandards Mobile Device Management sind zu beachten.[37]

**Kommentiert [FH27]:** Auf welcher Annahme basiert diese Einschränkung? M.E. ist nicht ersichtlich, warum für die Mitnutzung eines Cloud-Dienstes nicht ebenfalls die Erstellung eines Sicherheitskonzeptes notwendig sein sollte, insbesondere wenn die Bandbreite der extern verarbeitenden Daten nicht eingeschränkt ist. Sollte der Anwendungsfall „Mitnutzung" auf Grund des fehlenden Vertragsverhältnisses nicht genauso kritisch oder gar noch kritischer betrachtet werden als die „Nutzung"? Jede Art von Datenübertragung und Datenverarbeitung im Rahmen einer Nutzung oder Mitnutzung von Cloud-Diensten (selbst wenn es sich nur Metadaten handelt) sorgt für eine Vergrößerung des Angriffsvektors. Das spricht dafür, beim Szenario „Mitnutzung" mindestens dieselben Maßstäbe anzulegen (z.B. Kriterienkatalog C5) wie beim Szenario „Nutzung".

**Kommentiert [h8]:** Betrifft das Thema „Daten-Verschlüsselung" nur die Mitnutzung? Warum gilt es in diesem Mindeststandard nicht übergreifend für Nutzung und Mitnutzung?

[36] Hinweis: Ein Akzeptieren von Allgemeinen Geschäftsbedingungen (AGB) oder sonstigen Nutzungsbedingungen sind nicht als ein Vertragsverhältnis im Sinne dieses Mindeststands anzusehen.
[37] Siehe Mindeststandard des BSI Mobile Device Management, (BSI 2017), S.1ff.

# Literaturverzeichnis


AKTM (2011) Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, Orientierungshilfe – Cloud Computing, Version 2.0, Oktober 2014

BMI (2014) Bundesministerium des Innern, Erlass zur Verwendung einer Eigenerklärung und einer Vertragsklausel in Vergabeverfahren im Hinblick auf Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden, O4 - 11032/23#14, Berlin 2014

BMI (2017) Bundesministerium des Innern, für Bau und Heimat: Umsetzungsplan Bund 2017 – Leitlinie für die Informationssicherheit in der Bundesverwaltung

BMI (2018) Bundesministerium des Innern, für Bau und Heimat: Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), 10. August 2018

BSI (2008) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-4 – Notfallmanagement, Version 1.0

BSI (2017a) Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 200-2 – IT-Grundschutz-Methodik, Version 1.0

BSI (2017b) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI für Mobile Device Management, Version 1.0

BSI (2019) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandards – Antworten auf häufig gestellte Fragen zu den Mindeststandards, **Fehler! Linkreferenz ungültig.**~~https://www.bsi.bund.de/dok/11916758~~, abgerufen am 17.11.2020

BSI (2020a) Bundesamt für Sicherheit in der Informationstechnik: Kriterienkatalog Cloud Computing, Version 1.0 – Stand Februar 2020

BSI (2020b) Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, 3. Edition 2020

BSI (2020c) Bundesamt für Sicherheit in der Informationstechnik: Leitfaden mit Checkliste zur Auswertung einer Berichterstattung nach BSI C5, **Fehler! Linkreferenz ungültig.**~~https://www.bsi.bund.de/dok/14020574~~, abgerufen am 17.11.2020

DIN (2018) Deutsches Institut für Normierung e.V.: Normungsarbeit – Teil 2: Gestaltung von Dokumenten, DIN 820-2:2018-09

IETF (1997) Internet Engineering Task Force: Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, **Fehler! Linkreferenz ungültig.**~~https://tools.ietf.org/html/rfc2119~~, abgerufen am 17.11.2020

# Abkürzungsverzeichnis

| | |
|---|---|
| AGB | Allgemeine Geschäftsbedingungen |
| BMI | Bundesministerium des Innern, für Bau und Heimat |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| BSIG | Gesetz über das Bundesamt für Sicherheit in der Informationstechnik |
| BDSG | Bundesdatenschutzgesetz |
| C5 | Kriterienkatalog Cloud Computing |
| DIN | Deutsches Institut für Normierung e.V. |
| FAQ | Frequently Asked Questions |
| IETF | Internet Engineering Task Force |
| ISB | Informationssicherheitsbeauftragte |
| ISMS | Informationssicherheitsmanagementsystem |
| IT-SiBe | IT-Sicherheitsbeauftragte |
| StGB | Strafgesetzbuch |
| RFC | Request for Comments |
| VSA | Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA) |

| Seite 7: [1] Kommentiert [h3] | h726 | 10.12.2020 18:54:00 |
|---|---|---|

Der gesamte Abschnitt 2 sollte m.E. noch klarer zwischen Nutzung und Mitnutzung unterscheiden.

Bspw.:

Gilt wirklich nur Kapitel 2.5 für Mitnutzung-Dienste und gelten die Kapitel 2.1-2.4 nur für Nutzung-Dienste? Wenn ja, dann sollte das am Anfang von Abschnitt 2 klargestellt werden. Wenn Teile der Kapitel 2.1-2.4 auch für Mitnutzung-Dienste gelten, wäre das kenntlich zu machen.

Dass Kapitel 2.2 nur für Nutzung-Dienste gilt (weil diese mit Beschaffung und Beauftragung verbunden sind), leuchtet ein. Aber eine Planungsphase sollte es ggf. auch bei Mitnutzung-Diensten geben, wobei dabei vermutlich nicht das ganze Kapitel 2.1 zu beachten ist.

Grundsätzlich sei hier angemerkt, dass es sehr schlanke Mitnutzung-Möglichkeiten gibt, z.B. Cloud-Dienste, die im Internet leicht verfügbar und oftmals auch als freeware (ggf. mit Apache Lizenz, mit AGG, aber nicht unbedingt mit Vertrag – was ja dann keine Nutzung, sondern nur Mitnutzung ist) angeboten werden. Hierfür die gesamten Aufgaben aus Kap. 2.1 ff. abzuarbeiten, wäre ein unverhältnismäßiger und auch nicht erforderlicher Aufwand. Es sollte also insbesondere bei OSS darauf geachtet werden, dass Sicherheitsmaßnahmen ausreichend umgesetzt, aber keine übermäßigen konzeptionellen Aufwände für jeden kleinen Individualfall der Cloud-(Mit)Nutzung betrieben werden müssen.

Außerdem gibt es sicherlich auch schlanke Nutzung-Dienste. Hier ein Beispiel (mit der hypothetischen Annahme, dass es solch einen Service noch nicht als geeignete OSS gibt und folgende neue Beauftragung erfolgt): Eine Behörde beauftragt eine Firma mit der Entwicklung eines Wechselkursrechners, der an dem offiziellen Wechselkurs der betroffenen Nationalbanken orientiert ist. Die Firma entwickelt den Wechselkursrechner und bietet den Service in Form eines Cloud-Dienst eines externen Anbieters an. Die Behörde nimmt die Leistung auf Basis des mit der Firma geschlossenen Vertrages an. Die Behörde nutzt den Wechselkursrechner, indem sie Zahlenbeträge und die zugehörige Währung (dies sind die dienstlichen Daten) an den Wechselkursrechner sendet und den Zahlenbetrag in einer anderen Währung vom Cloud-Dienst zurückerhält. All das ist eng eingebunden in eine Fachanwendung der Behörde. Es werden keine personenbezogenen Daten gesendet.

- ➔ Für solch einen Anwendungsfall ist m.E. zu hinterfragen, ob es dafür wirklich eine Cloud-Strategie und ein für den Cloud-Dienst spezifisches eigenes Sicherheitskonzept geben muss. Den Service im Sicherheitskonzept der Fachanwendung zu erwähnen und dort die Abhängigkeiten zu dem externen Anbieter darzustellen, würde m.E. den Zweck ausreichend erfüllen.

| | |
|---|---|
| **Von:** | [redacted] /Z22 |
| **An:** | GP Mindeststandards Bund |
| **Cc:** | ISM |
| **Betreff:** | Mindeststandards nach § 8 BSIG, hier: Anmerkungen des BMBF zur RfC-Version 1.0.5 Externe Cloud-Dienste |
| **Datum:** | Dienstag, 24. November 2020 10:52:32 |
| **Anlagen:** | 20201123_BSI_Externe Cloud-Dienste.pdf |

Sehr geehrte Damen und Herren,

Bezug nehmend auf Ihr Schreiben vom 20.11.2020 zur Aktualisierung des Mindeststandards zur Nutzung externer Cloud-Dienste übermittle ich Ihnen die diesbezüglichen Anmerkungen des BMBF.

Mit freundlichen Grüßen

[redacted]

[redacted]
IT-Sicherheitsbeauftragter

_____
Referat Z22 - Informationstechnik

Bundesministerium für Bildung und Forschung

Heinemannstraße 2, 53175 Bonn | Postanschrift: 53170 Bonn
Tel.: +[redacted] | Fax: +[redacted] | [redacted]@bmbf.bund.de
www.bmbf.de | www.twitter.com/bmbf_bund | www.facebook.com/bmbf.de|
www.instagram.com/bmbf.bund

Bundesministerium
für Bildung
und Forschung

eu2020.de

**Der IT-Sicherheitsbeauftragte**

POSTANSCHRIFT Bundesministerium für Bildung und Forschung, 53170 Bonn

**Bundesamt für Sicherheit in der Informationstechnik**
Referat BL 35
55133 Bonn

Ausschließlich per E-Mail

HAUSANSCHRIFT Heinemannstraße 2, 53175 Bonn
POSTANSCHRIFT 53170 Bonn

TEL +49 (0)228 99 57-[redacted]
FAX +49 (0)228 99 57-8[redacted]
BEARBEITET VON [redacted]
E-MAIL [redacted]@bmbf.bund.de
HOMEPAGE www.bmbf.de

DATUM Bonn, den 23.11.2020

GZ 17502/1(2019) - 2020-45531
**(Bitte stets angeben)**

BETREFF **Mindeststandards nach § 8 BISG**
hier: Anmerkungen des BMBF zur RfC-Beta-Version 1.0.5 vom 17.112020 des Mindeststandards des BSI zur Nutzung externer Cloud-Dienste

BEZUG Ihr Schreiben vom 20.11.2020 (BL35 - 750 00 07)

Sehr geehrte Damen und Herren,

haben Sie vielen Dank für die Übersendung des bisherigen Entwurfs einer Überarbeitung des Mindeststandards des BSI zur Nutzung externer Cloud-Dienste sowie die damit verbundene Möglichkeit, im Rahmen des Konsultationsverfahrens eine Rückmeldung zu geben. Von dieser möchten wir in Bezug auf das mit dem Mindeststandard angesetzte Mindestsicherheitsniveau sowie auf das Verhältnis von Nutzung und Mitnutzung Gebrauch machen.

Sowohl in der aktuell gültigen Fassung, als auch im übermittelten Entwurf erscheint uns insbesondere die bedingungslose Verpflichtung zur Umsetzung und Einhaltung der Basiskriterien nach dem Kriterienkatalog Cloud Computing (C5) gemäß NCD.2.1.02 lit. b als ein zu enges Gewand, auf Grund dessen das Spannungsverhältnis zwischen Informationssicherheit und Anwenderfreundlichkeit nicht optimal austariert werden kann.

So hat zwar die Hinzuziehung des Kriterienkatalogs C5 zweifelsohne seine Berechtigung im Falle der Verarbeitung von Informationen, die einen hohen Schutzbedarf aufweisen oder als Verschlusssachen kategorisiert wurden. Auch sehen wir im Bereich sehr inhaltslastiger Cloud-Angebote wie z. B. im Falle des File Sharing oder einer weitreichenden Auslagerung der Datenverarbeitung zu Dienstleistern eine Notwendigkeit, die Anforderungen nach C5 oder die vertragliche Zusicherung von Gerichtstand, Lokation oder Datenrückgabe und Datenlöschung zu erfüllen. Jedoch gibt es mittlerweile diverse andere Cloud-Dienstleistungen wie bspw. Terminvereinbarungssysteme, Whiteboard-Lösungen oder virtuelle Lernwelten, über die Informationen ausgetauscht und verarbeitet werden, die regelmäßig keinen oder nur einen

geringen Schutzbedarf aufweisen. Da mit dem Mindeststandard in diesem Fall die Bestimmung des Sicherheitsniveaus relativ zum Schutzbedarf der Informationen ausgehebelt und dem Schutz mehr Wert beigemessen wird, als es die verarbeitete Information erfordert, muss oftmals auf die Nutzung eines Cloud-Anbieters verzichtet oder höhere Kosten in Kauf genommen werden. Die Verhältnismäßigkeit ist folglich nicht gewahrt.

Diese Problematik wurde augenscheinlich zumindest im Grunde erkannt und mit der Anforderung NCD.2.1.03 lit. e zu adressieren versucht. Allerdings wurde diese Anforderung so eng gefasst, dass hiesiger Auffassung nach als einziger Anwendungsfall die Verarbeitung privater Daten über dienstliche IT-Systeme verbleibt. Vor diesem Hintergrund schlagen wir vor, die Anforderung NCD.2.1.03 lit. e wie folgt zu ändern:

*Kommt die Einrichtung anhand der vorgenommenen Datenkategorisierung, der Schutzbedarfs- und der Risikoanalyse zu dem Ergebnis, dass in dem externen Cloud-Dienst ausschließlich Daten verarbeitet werden, die allenfalls einen geringen Schutzbedarf aufweisen und mit der Verarbeitung verbundene Restrisiken akzeptiert werden können, KANN die Einrichtung auf Sicherheitsanforderungen des Mindeststandards verzichten, die zur Erreichung des angestrebten Sicherheitsniveaus nicht erforderlich sind.*

Damit könnte ein höherer Flexibilisierungsgrad erreicht und das Verhältnis zwischen Nutzung und Mitnutzung stringenter ausgestaltet werden. Schließlich werden den Einrichtungen bei der Bewertung der Mitnutzung lediglich die Prüfkriterien vorgegeben. Hinsichtlich des Ergebnisses stehen ihnen jedoch weiterhin sämtliche Optionen offen. Diese größere Flexibilität bei der Mitnutzung kann dazu führen, dass Einrichtungen Cloud-Dienste, die die Vorgaben zur Nutzung nicht erfüllen können, über einen Dritten beauftragen und sich von diesem zur Mitnutzung einladen lassen. Sicherer wäre hingegen eine unmittelbare Einflussmöglichkeit auf den gebuchten Cloud-Dienst durch die Einrichtung, die mit dem oben gemachten Vorschlag erreicht werden könnte, auch wenn bspw. der Dienstleister über kein C5-Testat verfügt oder eine Vertraulichkeitsvereinbarung nach NCD.2.2.05 lit. a nicht zusichern kann.

Da das BMBF im Vergleich zu anderen Ressorts überdurchschnittlich häufig mit externen Entitäten wie z. B. Forschungseinrichtungen, Projektträgern oder Konsortien zusammenarbeitet und diese im Kern unseren Geschäftsbereich darstellen, sind wir in besonderem Maße auf diese Flexibilität bei der Auswahl von Cloud-Diensten angewiesen. Dies bitten wir zu berücksichtigen.

Mit freundlichen Grüßen
Im Auftrag

gez. [redacted]

| | |
|---|---|
| **Von:** | [redacted] im Auftrag von KdoCIR FaeEntw-InfoSichh |
| **An:** | GP Mindeststandards Bund |
| **Cc:** | FKT-BMVg CIT II 2 |
| **Betreff:** | AW: : [MST NCD] Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2.0 |
| **Datum:** | Freitag, 8. Januar 2021 12:58:06 |
| **Anlagen:** | image002.png<br>image003.png<br>image005.jpg<br>MST-NCD-RfC-Beta-1.0.5_BMVg.docx |

---

Sehr geehrte Damen und Herren,

herzlichen Dank für die Beteiligung an der Erarbeitung des Mindeststandards.
Im Auftrag des BMVg habe ich die Mitprüfung in Federführung übernommen.
Für das Verteidigungsressort bitte ich, die Anmerkungen siehe Anlage zu berücksichtigen. Eine entsprechende Erläuterung ist ebenfalls enthalten.

Bei Fragen stehe ich Ihnen gern zur Verfügung.

Mit freundlichem Gruß,
im Auftrag

[redacted]
Oberstleutnant
Referent IT-Grundschutz

Kommando Cyber- und Informationsraum
Ref Informationssicherheit I 5

Johanna-Kinkel-Straße 2-
4 | D 53175 Bonn
Büro: Etage 2 Raum C.3.10

Telefon: +[redacted]
E-Mail: [redacted]@bundeswehr.org
[redacted]-
[redacted]@bundeswehr.org
Internet:
Twitter: https://cir.bundeswehr.de
https://twitter.com/cirbw

----- Weitergeleitet von [redacted]/BMVg/BUND/DE am 20.11.2020 11:07 -----

Von: "GP Geschaeftszimmer_BL" <geschaeftszimmer-bl@bsi.bund.de>
An: "poststelle@bk.bund.de" <poststelle@bk.bund.de>, "poststelle@auswaertiges-amt.de" <poststelle@auswaertiges-amt.de>, "poststelle@bmi.bund.de" <poststelle@bmi.bund.de>, "poststelle@bmf.bund.de" <poststelle@bmf.bund.de>, "poststelle@bmjv.bund.de" <poststelle@bmjv.bund.de>, "poststelle@bmvg.bund.de" <poststelle@bmvg.bund.de>, "info@bmwi.bund.de" <info@bmwi.bund.de>, "poststelle@bmas.bund.de" <poststelle@bmas.bund.de>, "poststelle@bmel.bund.de" <poststelle@bmel.bund.de>, "poststelle@bmfsfj.bund.de" <poststelle@bmfsfj.bund.de>, "poststelle@bmg.bund.de" <poststelle@bmg.bund.de>, "poststelle@bmvi.bund.de" <poststelle@bmvi.bund.de>, "Poststelle@bmu.bund.de" <Poststelle@bmu.bund.de>,

"information@bmbf.bund.de" <information@bmbf.bund.de>, "poststelle@bmz.bund.de" <poststelle@bmz.bund.de>, "bverfg@bundesverfassungsgericht.de" <bverfg@bundesverfassungsgericht.de>, "poststelle@bpra.bund.de" <poststelle@bpra.bund.de>, "bundesrat@bundesrat.de" <bundesrat@bundesrat.de>, "Poststelle@brh.bund.de" <Poststelle@brh.bund.de>, [redacted]@bundestag.de" <[redacted]@bundestag.de>, "Poststelle@bkm.bund.de" <Poststelle@bkm.bund.de>, "Poststelle@bfdi.bund.de" <Poststelle@bfdi.bund.de>, [redacted]@itzbund.de" [redacted]@itzbund.de>, [redacted]@jm.nrw.de" [redacted]@jm.nrw.de>, "GP AG-InfoSic" [redacted]@bsi.bund.de>

Kopie: "GP Abteilung BL" <abteilung-bl@bsi.bund.de>, "GP Fachbereich BL 3" <fachbereich-bl3@bsi.bund.de>, "GP Referat BL 35" <referat-bl35@bsi.bund.de>, "GP Poststelle" <poststelle@bsi.bund.de>, "GP Stab 3 - Strategie und Leitungsunterstuetzung" <stab3@bsi.bund.de>, "GP Geschaeftszimmer_BL" <geschaeftszimmer-bl@bsi.bund.de>

Datum: 20.11.2020 11:06

Betreff: [MST NCD] Mindeststandard zur Nutzung externer Cloud-Dienste, hier: Konsultationsverfahren zum Major-Release Version 2.0

Gesendet von: "[redacted]" <[redacted]@bsi.bund.de>

---

Sehr geehrte Damen und Herren,

anbei übersende ich Ihnen das Anschreiben sowie den Mindeststandard des BSI zur Nutzung externer Cloud-Dienste nach § 8 Absatz 1 Satz 1 BSIG - RfC-Beta-Version 1.0.5 vom 17.11.2020. Die Abgleichstabelle zum Mindeststandard ist der E-Mail ebenfalls beigefügt.

Mit freundlichen Grüßen
Im Auftrag

[redacted]

---

Geschäftszimmer BL
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 228 99 9582-[redacted]
Fax: +49[redacted] 99 10 9582[redacted]
E-Ma[redacted]
geschaeftszimmer-bl@bsi.bund.de
Internet: www.bsi.bund.de

www.bsi-fuer-buerger.de

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

# Mindeststandard des BSI zur Nutzung externer Cloud-Dienste

nach § 8 Absatz 1 Satz 1 BSIG – RfC-Beta-Version 1.0.5 vom 17.11.2020

# Änderungshistorie

| *Version* | *Datum* | *Beschreibung* |
|---|---|---|
| 1.0 | 24.04.2017 | Erstveröffentlichung |
| 1.0.1 | 13.07.2020 | RfC-Alpha-Version, Rohentwurf auf Basis der Delta-Dokumentation |
| 1.0.2 | 25.09.2020 | Prüfung, Überarbeitung und Freigabe durch Fachreferat |
| 1.0.3 | 29.09.2020 | RfC-Alpha-Version zur hausinternen Abstimmung |
| 1.0.4 | 09.11.2020 | Kommentare und Rückmeldungen aus der hausinternen Abstimmung eingearbeitet |
| 1.0.5 | 17.11.2020 | Ressorts erhalten Entwurf zur Kommentierung |

Tabelle 1: Versionsgeschichte des Mindeststandards. Eine ausführliche Änderungsübersicht zum Mindeststandard erhalten Sie unter: https://www.bsi.bund.de/mindeststandards (**Hinweis:** wird vor Release konkretisiert)

**Feldfunktion geändert**

Bundesamt für Sicherheit in der Informationstechnik Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6262
E-Mail: mindeststandards@bsi.bund.de
Internet: https://www.bsi.bund.de

# Vorwort

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes auf der Grundlage des § 8 Abs. 1 BSIG. Als gesetzliche Vorgabe definieren Mindeststandards ein konkretes Mindestniveau für die Informationssicherheit. Der Umsetzungsplan Bund 2017 legt fest, dass die Mindeststandards des BSI auf Basis § 8 Abs. 1 BSIG zu beachten sind.[1] Die Definition erfolgt auf Basis der fachlichen Expertise des BSI in der Überzeugung, dass dieses Mindestniveau in der Bundesverwaltung nicht unterschritten werden darf. Der Mindeststandard richtet sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe)[2] und IT-Betriebspersonal.

IT-Systeme sind in der Regel komplex und in ihren individuellen Anwendungsbereichen durch die unterschiedlichsten (zusätzlichen) Rahmenbedingungen und Anforderungen gekennzeichnet. Daher können sich in der Praxis regelmäßig höhere Anforderungen an die Informationssicherheit ergeben, als sie in den Mindeststandards beschrieben werden. Aufbauend auf den Mindeststandards sind diese individuellen Anforderungen in der Planung, der Etablierung und im Betrieb der IT-Systeme zusätzlich zu berücksichtigen, um dem jeweiligen Bedarf an Informationssicherheit zu genügen. Die Vorgehensweise dazu beschreiben die IT-Grundschutz-Standards des BSI.

Zur Sicherstellung der Effektivität und Effizienz in der Erstellung und Betreuung von Mindeststandards arbeitet das BSI nach einer standardisierten Vorgehensweise. Zur Qualitätssicherung durchläuft jeder Mindeststandard mehrere Prüfzyklen einschließlich des Konsultationsverfahrens mit der Bundesverwaltung.[3] Über die Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich jede Stelle des Bundes auch bei der Erschließung fachlicher Themenfelder für neue Mindeststandards einbringen oder im Hinblick auf Änderungsbedarf für bestehende Mindeststandards Kontakt mit dem BSI aufnehmen. Einhergehend mit der Erarbeitung von Mindeststandards berät das BSI die Stellen des Bundes[4] auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Vgl. Umsetzungsplan Bund 2017 (BMI 2017), S. 4
[2] Analog „Informationssicherheitsbeauftragter (ISB)“
[3] Siehe FAQ zu den Mindeststandards (BSI 2020)
[4] Zur besseren Lesbarkeit wird im weiteren Verlauf für „Stelle des Bundes“ der Begriff „Einrichtung“ verwendet.

# Inhalt



Feldfunktion geändert

# 1 Beschreibung

Dieser Mindeststandard setzt Sicherheitsanforderungen an die Nutzung externer Cloud-Dienste. Die Erfüllung der im Mindeststandard vorgegebenen Sicherheitsanforderungen ist für ein angemessenes IT-Sicherheitsniveau notwendig, aber in der Regel nicht hinreichend. Unter Berücksichtigung des individuellen Schutzbedarfs muss die Festlegung und Umsetzung eventuell zusätzlich erforderlicher Sicherheitsanforderungen erfolgen. Er richtet sich hinsichtlich seiner Umsetzung an IT-Sicherheitsbeauftragte, IT-Betriebs- und Fachverantwortliche.[5]

## 1.1 Begriffsbestimmung und Abgrenzung

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Insbesondere werden dabei Infrastrukturen, Plattformen und Software angeboten, die Spannbreite der angebotenen Cloud-Dienste umfasst darüber hinaus jedoch das komplette Spektrum der Informationstechnik.[6]

Externe Cloud-Dienste im Sinne dieses Mindeststandards sind im Rahmen von Cloud Computing angebotene Dienstleistungen, die über Netze und Anbieter der Wirtschaft außerhalb der öffentlichen Verwaltung des Bundes und der Länder erbracht werden.[7] Nutzt die öffentliche Verwaltung jedoch ihrerseits externe Cloud-Dienste, so ist der hier dargestellte Mindeststandard ebenfalls einzuhalten.

Als Nutzung ist eine Verarbeitung von dienstlichen Daten[8] durch einen externen Cloud-Dienst zu verstehen, der durch die Einrichtung selbst oder gemeinsam mit anderen beauftragt wird. Werden externe Cloud-Dienste durch Benutzer[9] einer Einrichtung lediglich mitgenutzt, regelt Kapitel 2.5 den Umgang mit dienstlichen Daten in diesen Fällen entsprechend. Von einer Mitnutzung wird insbesondere ausgegangen, wenn die Einrichtung den externen Cloud-Dienst~~en~~ nicht beauftragt hat.

Werden keine dienstlichen Daten verarbeitet, können die Regelungen des Mindeststandards trotzdem angewendet werden (siehe NCD.2.1.03, Buchstabe e)).

## 1.2 Modalverben

In Anlehnung an den IT-Grundschutz[10] werden die Sicherheitsanforderungen mit den Modalverben MUSS und SOLLTE sowie den zugehörigen Verneinungen formuliert. Darüber hinaus wird das Modalverb KANN für ausgewählte Prüfaspekte verwendet. Die hier genutzte Definition basiert auf RFC 2119[11] und DIN 820-2: 2018[12].

**MUSS / DARF NUR**

bedeutet, dass diese Anforderung zwingend zu erfüllen ist. Das von der Nichtumsetzung ausgehende Risiko kann nicht im Rahmen einer Risikoanalyse akzeptiert werden.

**DARF NICHT / DARF KEIN**

[5] Rollen nach IT-Grundschutz-Kompendium, (BSI 2020b), S.31
[6] Definition nach https://www.bsi.bund.de/cloud
[7] Hinweis: IT-Dienstleistungen der „Bundescloud“ und alle durch DLZ IT des Bundes aus einer Private Cloud (z. B. pCloudBw) erbrachten IT-Dienstleistungen in den Bundes- und Landesressorts fallen somit nicht unter diese Bestimmung.
[8] Dienstlich sind alle Daten, die im Rahmen der dienstlichen Tätigkeit erhoben und verarbeitet werden. Darunter fallen jedoch nicht personenbezogene Daten (wie Stammdaten, Nutzungsdaten), die für die Registrierung und Nutzung des Dienstes vom Cloud-Diensteanbieter erhoben oder verarbeitet werden.
[9] Analog Rolle „Benutzer“ nach IT-Grundschutz-Kompendium, (BSI 2020b), S.31
[10] Vgl. BSI-Standard 200-2 (BSI 2017), S. 18
[11] Vgl. Key words for use in RFCs (IETF 1997)
[12] Vgl. DIN-820-2: Gestaltung von Dokumenten (DIN 2018)

**Kommentiert [RKP1]:** BAAINBw I2.4: Das IT-Systemhaus der Bw (BWI) ist als dem BMVg zugehörige Einheit kein externer Cloud-Dienstleister.

**Kommentiert [GJ2]:** BAAINBw I3: siehe Fußnote: die neu eingefügte Fußnote greift h.E. zu kurz: insbesondere die pCloudBw („on-premises“ betrieben durch die BWI als DLZ-IT des Bundes) ist ebenfalls auszunehmen. Darüber hinaus werden DLZ-IT auch ihrerseits externe Cloud-Dienste („off-premises“) nutzen. Diese Leistungen unterfallen dann wieder den hier dargestellten Mindeststandards.

**Feldfunktion geändert**

bedeutet, dass etwas zwingend zu unterlassen ist. Das durch die Umsetzung entstehende Risiko kann nicht im Rahmen einer Risikoanalyse akzeptiert werden.

**SOLLTE**

bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

**SOLLTE NICHT / SOLLTE KEIN**

bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

**KANN**

bedeutet, dass die Umsetzung / Nicht-Umsetzung optional ist und ohne Angabe von Gründen unterbleiben kann.

# 2 Sicherheitsanforderungen

Nachfolgende Sicherheitsanforderungen adressieren die Informationssicherheit entlang des gesamten Lebenszyklus und setzen auf den IT-Grundschutz-Baustein OPS.2.2 *Cloud-Nutzung*[13] auf.

## 2.1 Planungsphase

Grundlage der Informationssicherheit im Bereich Cloud Computing bilden nach dem IT-Grundschutz-Baustein OPS.2.2: *Cloud-Nutzung*

- die Cloud-Nutzungs-Strategie
- die darauf basierende Sicherheitsrichtlinie sowie
- das jeweilige Sicherheitskonzept für den externen Cloud-Dienst.

Die nachfolgenden Sicherheitsanforderungen adressieren diese Dokumente entsprechend.

**NCD.2.1.01 Cloud-Nutzungs-Strategie**

a) Die Einrichtung MUSS prüfen, ob der externe Cloud-Dienst grundsätzlich mit den in der Cloud-Nutzungs-Strategie definierten Zielen, Chancen und Risiken vereinbar ist.[14]

b) Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn Ziele, Chancen und Risiken der Cloud-Nutzungs-Strategie angemessen berücksichtigt werden können.

**NCD.2.1.02 Sicherheitsrichtlinie externe Cloud-Dienste**

a) Die Einrichtung MUSS eine Sicherheitsrichtlinie für externe Cloud-Dienste nach OPS.2.2.A2 *Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung*[15] erstellen.

b) Die Einrichtung MUSS in dieser Sicherheitsrichtlinie mindestens die Umsetzung und Einhaltung der Basiskriterien nach dem Kriterienkatalog Cloud Computing (C5) als spezielle Sicherheitsanforderungen an den Cloud-Diensteanbieter festlegen.[16]

c) Die Einrichtung MUSS die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragen bei der Erstellung der Sicherheitsrichtlinie beteiligen.

**NCD.2.1.03 Sicherheitskonzept für den externen Cloud-Dienst**

a) Die Einrichtung MUSS ein Sicherheitskonzept für den externen Cloud-Dienst nach OPS.2.2.A7 *Erstellung eines Sicherheitskonzeptes für die Cloud-Nutzung* erstellen.

b) Die Einrichtung MUSS in dem Sicherheitskonzept die aktuellen Veröffentlichungen des BSI zu Cloud-Sicherheit berücksichtigen.[17]

c) Die Einrichtung MUSS die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragen bei der Erstellung des Sicherheitskonzeptes beteiligen.

d) Die Einrichtung MUSS eine Datenkategorisierung durchführen, in der sämtliche dienstliche Daten identifiziert werden, die künftig in dem externen Cloud-Dienst verarbeitet werden sollen.

[13] IT-Grundschutz-Kompendium, (BSI 2020b), OPS.2.2: *Cloud-Nutzung*
[14] Hinweis: OPS.2.2.A1 *Erstellung einer Cloud-Nutzungs-Strategie* sieht die Erstellung einer Cloud-Nutzungs-Strategie vor. In dieser erfasst die Einrichtung ihre Ziele, Chancen und Risiken, die sie mit einer Cloud-Nutzung generell verbindet. Die Cloud-Nutzungs-Strategie nimmt daher eine zentrale Rolle für die Einrichtung ein. Sie wird benötigt, um die beabsichtigte Nutzung eines konkreten externen Cloud-Dienstes bewerten zu können.
[15] IT-Grundschutz-Kompendium, (BSI 2020b), OPS.2.2: *Cloud-Nutzung*
[16] Kriterienkatalog Cloud Computing (C5), (BSI 2020a), S.1ff.
[17] Siehe Veröffentlichungen unter https://www.bsi.bund.de/cloud

Feldfunktion geändert

e) Kommt die Einrichtung zu dem Ergebnis, dass in dem externen Cloud-Dienst keine dienstlichen Daten verarbeitet werden, handelt es sich nicht um eine Nutzung oder Mitnutzung externer Cloud-Dienste im Sinne dieses Mindeststandards. In diesem Fällen KANN die Einrichtung die Sicherheitsanforderungen des Mindeststandards umsetzen.

f) Die Einrichtung MUSS für die identifizierten dienstlichen Daten Geheim- und Datenschutzaspekte[18] sowie Personen- und Dienstgeheimnisse ermitteln.

g) Die Einrichtung MUSS die identifizierten dienstlichen Daten den nachfolgenden Kategorien zuordnen:

- Kategorie 1 = Privat- und Dienstgeheimnisse gemäß §§ 203 und 353b StGB
- Kategorie 2 = personenbezogene Daten gemäß § 3 Absatz 1 BDSG
- Kategorie 3 = Verschlusssachen gemäß Verschlusssachenanweisung - VSA[19]
- Kategorie 4 = sonstige Daten (weder Kategorie 1, noch 2, noch 3)

h) Die Einrichtung KANN die identifizierten dienstlichen Daten den Kategorien 1, 2 oder 3 gleichzeitig zuordnen.

i) Die Einrichtung MUSS Risiken, die aus der künftigen Nutzung des externen Cloud-Dienstes entstehen können, umfassend ermitteln.[20]

i) Die Einrichtung MUSS die ermittelten Risiken mit denen in der eigenen Cloud-Nutzungs-Strategie (siehe NCD.2.1.01) festgelegten Richtlinien der Risikobewertung abgleichen und bewerten.

ii) Die Einrichtung DARF den externen Cloud-Dienst NUR nutzen, wenn die ermittelten Risiken gemäß der in der Cloud-Nutzungs-Strategie genannten Richtlinien zur Risikobewertung wirksam vermieden oder hinreichend reduziert oder getragen werden können.

**NCD.2.1.04 Notfall- und Kontinuitätsmanagement**

Mit Notfall- bzw. Kontinuitätsmanagement ist gemäß BSI-Standard 100-4[21] ein Managementsystem zur Aufrechterhaltung einer definierten Arbeitsfähigkeit einer Einrichtung gemeint und umfasst sowohl präventive als auch reaktive Maßnahmen auf Notfälle und Krisensituationen. Es gilt im weiteren die Begrifflichkeit des BSI-Standards 100-4[22].

a) Die Einrichtung MUSS prüfen, ob sie in Notfällen und Krisensituationen weiter auf den externen Cloud-Dienst zugreifen können muss. [23]

b) Die Einrichtung MUSS bewerten, welche Bedeutung der externe Cloud-Dienst in Notfällen einnehmen würde.[24]

[18] Hinsichtlich Datenschutzaspekte siehe insbesondere (AKTM 2011), S.1ff.
[19] Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA), (BMI 2018)
[20] Hinweis: Bei dieser Prüfung geht es um eine anbieterunabhängige Prüfung. Es soll in diesem Zusammenhang geklärt werden, ob das beabsichtigte Cloud-Szenario mit der Cloud-Nutzung-Strategie vereinbar ist (z.B. Können die eigenen rechtlichen und organisatorischen Rahmenbedingungen überhaupt erfüllt werden?)
[21] BSI-Standard 100-4 – Notfallmanagement, (BSI 2008), S.1ff.
[22] BSI-Standard 100-4 – Notfallmanagement, (BSI 2008), S.1ff.
[23] Hinweis: Leitfragen für diese Prüfung können sein: Wird der Cloud-Dienst für einen, im Notfallmanagement als zeitkritisch bewerteten Geschäftsprozess (bzw. Fachaufgabe) genutzt? Dient der Cloud-Dienst zur Etablierung und Aufrechterhaltung eines Notbetriebs? Ist der Cloud-Dienst für die Bewältigung eines Notfalls relevant?
[24] Hinweis: Leitfragen für diese Prüfung können sein: Wie zeitkritisch sind die Geschäftsprozesse (bzw. Fachaufgaben), die den Cloud-Dienst in einem Notfall oder einer Krise benötigen? Zu welchem Grad wird der Cloud-Dienst in einem Notbetrieb benötigt?